

A Multilevel Framework for Lattice Network Coding

Yi Wang, Alister Burr, Qinhui Huang and Mehdi Molu

Abstract

We present a general framework for studying the multilevel structure of lattice network coding (LNC), which serves as the theoretical fundamental for solving the ring-based LNC problem in practice, with greatly reduced decoding complexity. Building on the framework developed, we propose a novel lattice-based network coding solution, termed layered integer forcing (LIF), which applies to any lattices having multilevel structure. The theoretic foundations of the developed multilevel framework lead to a new general lattice construction approach, the elementary divisor construction (EDC), which shows its strength in improving the overall rate over multiple access channels (MAC) with low computational cost. We prove that the EDC lattices subsume the traditional complex construction approaches. Then a soft detector is developed for lattice network relaying, based on the multilevel structure of EDC. This makes it possible to employ iterative decoding in lattice network coding, and simulation results show the large potential of using iterative multistage decoding to approach the capacity.

I. INTRODUCTION

There has recently been a resurgence in research on lattice codes for wireless communications, as a result of two recent developments. The first is recent work [1, 2] which has shown that lattice codes with lattice decoding are capable of approaching channel capacity. The second is their application to physical layer network coding (PNC) [3] for ultra-dense wireless multihop networks [4]. In particular Nazer and Gastpar have developed compute-and-forward (C&F) [5], which applies structured nested lattice codes to PNC for multiuser relay networks. However it is difficult to increase the transmission rate using previous lattice constructions such as construction A lattices, since this requires linear channel codes over large finite fields, for which the decoding complexity is typically unaffordable. This paper lays the foundations for a multilevel structure for lattice codes, and uses it to introduce a general lattice construction approach and two multistage decoding approaches which greatly simplify decoding, and which can exploit iterative techniques to approach capacity.

Feng *et al.* formulated a general algebraic framework for lattice network coding (LNC) [6], giving practical design guidelines for C&F. Previous work, e.g. in [6–8], has given LNC design guidelines when

The work described in this paper was supported by the European Commission Framework 7 Programme under grant agreement 318177 (DIWINE).

quotient lattices are constructed from existing channel codes using complex construction A. In this paper, we consider a multilevel structure for lattice network coding, which provides a practical solution to the ring-based network coding problem. We also propose an efficient lattice construction approach (which we term the elementary divisor construction (EDC)) based on the theorems developed, which also subsumes the most important previous lattice constructions. The EDC lattice has a multilevel algebraic structure, and is well suited for multistage decoding. Note that the recently proposed product construction [9] used in C&F is a special case of EDC. The EDC approach is a straightforward result of the theoretic framework developed in section III. We give explicit representation of the generator matrix for the EDC lattice, propose a new concept of the primary sublattice, and derive the nominal coding gain and kissing numbers for the EDC lattice in all forms. The main contributions of the paper are summarised below:

- 1) We develop a generic multilevel lattice network coding scheme based on some algebraic theorems. This approach keeps beneficial compatibility of the traditional LNC scheme, whereas enabling more flexible coding design techniques. Note that MLNC makes also no particular assumption about the structure of the underlying nested lattice code.
- 2) We propose a novel lattice network decoding approach based on MLNC, termed layered integer forcing (LIF), which
 - improves the overall throughput for network coding with greatly reduced decoding complexity.
 - decodes lattices which are no longer a vector space.
 - allows flexible linear labelling design for additional performance enhancement.
- 3) We develop a modified Viterbi algorithm which implements LIF.
- 4) Building on the algebraic framework developed for MLNC, we present a novel lattice construction approach (EDC approach), show its good structure properties (e.g. the explicit form of the generator matrix) in reducing the decoding complexity, and derive its nominal coding gain and kissing numbers. Mathematically we also prove that EDC lattices subsume the most important complex lattice constructions.
- 5) We propose a soft detector specifically designed for EDC lattices (as an alternative to LIF for decoding EDC lattices). We evaluate its non-binary extrinsic information transfer characteristics, and propose an iterative multistage decoding approach for EDC lattices, which shows a substantial improvement in decoding performance.
- 6) We show how multistage detection, iteration-aided multistage detection, and LIF can be applied to MLNC. We also show, by simulation, that iterative decoding performs better than the Viterbi

detection approach used in the traditional LNC. This provides the basis for further work, and opens a new research area of iterative decoding for lattice network coding.

This paper lays the foundations for a new research area in multistage and iterative decoding for lattice network coding. We expect that it will provide the basis for extensive further work, both to explore the rich algebraic features of the new construction, and to exploit it in practical implementations of LNC in 5G wireless systems.

The remainder of this paper is organised as follows. In section II we review some algebraic preliminaries which will be useful in setting up our multilevel framework. Section III studies the algebraic properties of MLNC and presents the practically feasible encoding and decoding solutions. Section IV presents a new general lattice construction approach based on MLNC theorems developed and proves that it subsumes some important lattice constructions that have been widely known. Section V presents the soft detector for MLNC and studies the iterative decoding and multistage decoding approaches designed for MLNC. Section VI presents the simulation results based on different decoding modes. Section VII concludes the paper and presents the future work.

A. Notations

Notations used throughout this paper are defined as follows. \mathbb{N} , \mathbb{Z} and \mathbb{C} denote the fields of natural numbers, integers and complex numbers, respectively. \mathbb{F}_q , $q > 1$, $q \in \mathbb{Z}$ denotes the finite field of size q . \mathbb{F}_q^n denotes an n -tuple finite field where the field size for the i^{th} dimension $i \in \{1, 2, \dots, n\}$ is determined by $q_i \in \mathbb{Z}$. We also use boldface lower-case to denote a vector, i.e. $\mathbf{a} = [a^1, a^2, \dots, a^n]$. $\mathbf{V}^{\setminus i} \triangleq [V^1, V^2, \dots, V^{i-1}, V^{i+1}, \dots, V^n]$ represents a set including all elements except the i^{th} one. The upper-case letter (e.g. V) represents a random variable and its realisation is denoted by the lower-case v . The direct sum and direct product are denoted as \oplus and \times , respectively.

II. ALGEBRA PRELIMINARIES

We present some definitions and theorems in abstract algebra, which can be found in relevant textbooks, e.g. [10].

A. Ideal and Principal Ideal Domain

Let R be a commutative ring with identity 1, and $R^* = R \setminus 0$. A *unit* $\mathcal{U}(R)$ in R refers to any element x in R such that $xr = rx = 1$ for some $r \in R$. Any root of unity in a ring R is a unit. An element x in R is called a *zero divisor* $\mathcal{Z}(R)$ if $xr = rx = 0$ for some $r \in R^*$. An element $p \in R$, $p \notin \mathcal{Z}(R)$, $p \notin \mathcal{U}(R)$, is called a *prime* in R when $p \mid ab$ for some $a, b \in R^*$, then either $p \mid a$ or $p \mid b$.

An *ideal* \mathcal{I} of R is a non-empty subset of R that is closed under subtraction (which implies that \mathcal{I} is a group under addition), and is defined by:

$$1) \quad \forall a, b \in \mathcal{I}, a - b \in \mathcal{I}.$$

$$2) \quad \forall a \in \mathcal{I}, \forall r \in R, \text{ then } ar \in \mathcal{I} \text{ and } ra \in \mathcal{I}.$$

If $A = \{a_1, \dots, a_m\}$ is a finite non-empty subset of R , we use $\langle a_1, \dots, a_m \rangle$ to represent the ideal generated by A , i.e.

$$\langle a_1, \dots, a_m \rangle = \{a_1 r_1 + \dots + a_m r_m : r_1, \dots, r_m \in R\}$$

Note that R has at least two ideals $\{0\}$ and $\{R\}$.

An ideal \mathcal{I} of R is said to be *proper* if and only if $1 \notin \mathcal{I}$. An ideal \mathcal{I}_{\max} is said to be *maximal* if \mathcal{I}_{\max} is a proper ideal and the only ideals that include \mathcal{I}_{\max} are R and \mathcal{I}_{\max} itself. We say that an equivalence relation $a \sim b$ on the set R is defined by \mathcal{I} if and only if $a - b \in \mathcal{I}$.

An ideal \mathcal{I} of R is *principal* if \mathcal{I} is generated by a single element $a \in \mathcal{I}$, written as $\mathcal{I} = \langle a \rangle$. A *principal ideal ring* is a ring whose every ideal is principal. If R is a principal ideal ring without zero divisors, then R forms an ideal domain, and more precisely, a *principal ideal domain* (PID). Examples of PIDs include the ring of integers, the ring of Gaussian integers $\mathbb{Z}[i]$ and the ring of Eisenstein integers $\mathbb{Z}[\omega]$.

B. Modules over PID and Structure Theorem

Again, let S be a commutative ring with identity 1. An S -module M over S is an abelian group $(M, +)$ under a binary operation $+$, together with a function $\mathcal{F} : S \times M \mapsto M$ which satisfies the same conditions as those for vector space. Note that modules over a field are the same as vector spaces. An S -submodule of M is a subgroup N of M which is closed under the action of ring elements, and hence the submodule N forms also an S -module under the restricted operations.

An S -module is said to be finitely generated (f.g.) if M has a finite basis $\{m_1, \dots, m_n\}$ such that $\sum_i Rm_i = M$.

The annihilator of an element $m \in M$ is the set of elements $s \in S$ such that $sm = 0$. The annihilator of M is the elements $s \in S$ such that $\{sm = 0 | m \in M\}$, denoted by $\text{Ann}_S(M) = \bigcap \{\text{Ann}_S(m) | m \in M\}$. If M is a free S -module, then $\text{Ann}_S(M) = \langle 0 \rangle$.

If M is annihilated by ideal \mathcal{I} of S , we can make M into a quotient S -module M/N by defining an action on M satisfying,

$$m(s + \mathcal{I}) = ms, \quad \forall m \in M$$

The torsion submodule M_{Tor} of M is defined by:

$$M_{\text{Tor}} = \{m \in M : \text{Ann}_S(m) \neq \{0\}\}$$

A torsion free module is trivial.

Let M and N be two S -modules. An S -module homomorphism is a map $\phi : M \mapsto N$, which respects the S -module structures of M and N , i.e.,

$$\phi(s_1 m_1 + s_2 m_2) = s_1 \phi(m_1) \odot s_2 \phi(m_2)$$

$\forall s_1, s_2 \in S, \forall m_1, m_2 \in M$. An S -module homomorphism $\phi : M \mapsto N$ is called an S -module isomorphism if it is both injective and surjective, which is denoted by $M \cong N$. The kernel of ϕ denotes the elements in M which makes the image of ϕ equal to zero.

III. MULTILEVEL LATTICE NETWORK CODING

A. Algebraic Approach for Multilevel Structure

Briefly if there is a matrix $\mathbf{G}_\Lambda \in \mathbb{C}^{n' \times n}$, $n' \leq n$ such that all its n' row vectors $\mathbf{g}_{\Lambda,1}, \dots, \mathbf{g}_{\Lambda,n'} \in \mathbb{C}^n$ are linearly independent, the set of all S -linear combinations of $\mathbf{g}_{\Lambda,1}, \dots, \mathbf{g}_{\Lambda,n'}$ forms an S -lattice $\Lambda \in \mathbb{C}^n$, written by, $\Lambda = \{\mathbf{s}\mathbf{G}_\Lambda : \mathbf{s} \in S^{n'}\}$, where \mathbf{G}_Λ is called the lattice generator.

Following the explanation in section II-B, an n -dimensional S -lattice is precisely an S -module over PID, and similarly the sublattice Λ' in Λ forms a S -submodule. The partition of the S -lattice, denoted by Λ/Λ' represents $|\Lambda : \Lambda'| < \infty$ (the index of Λ') equivalence classes. Assume S is a PID, we have the following theorem.

Theorem 1: Let Λ and Λ' be S -lattices and S -sublattices, $\Lambda' \subseteq \Lambda$, $|\Lambda : \Lambda'| < \infty$ such that Λ/Λ' has nonzero annihilators. Then Λ/Λ' is the direct sum of a finite number of quotient sublattices,

$$\Lambda/\Lambda' = \Lambda_{p_1}/\Lambda'_{p_1} \oplus \Lambda_{p_2}/\Lambda'_{p_2} \oplus \dots \oplus \Lambda_{p_m}/\Lambda'_{p_m} \quad (1)$$

where $\Lambda_{p_i}/\Lambda'_{p_i} \triangleq \{\lambda \in \Lambda/\Lambda' : p_i^\gamma \lambda = 0\}$ for some $\gamma \geq 1$, and every $p_i, i = 1, 2, \dots, m$ is a distinct prime over S .

Proof: The quotient S -lattice Λ/Λ' has non-zero annihilators; this implies that Λ/Λ' forms a $f.g.$ torsion module. Let $\lambda \in \Lambda/\Lambda'$ and suppose that $\text{Ann}_S(\Lambda/\Lambda') = Sa$, where $a \in S$ and $a \neq 0$ (the property of the torsion module). Since S is also a unique factorization domain, so $a = p_1^{\gamma_1} p_2^{\gamma_2} \dots p_m^{\gamma_m}$. We now write $a_i = a/p_i^{\gamma_i}$ which is the product of irreducible factors that are relatively prime to p_i . There must

exist s_1, s_2, \dots, s_m in S such $\sum_{i=1}^m s_i a_i = 1$ since $\gcd(a_1, a_2, \dots, a_m) = 1$; Now we have

$$s_i p_i^{\gamma_i} a_i \lambda = 0 \quad (2)$$

since a annihilates Λ/Λ' . Theorem 1 states that the sublattice $\Lambda_{p_i}/\Lambda'_{p_i}$ must satisfy the condition $p_i^{\gamma_i} \lambda = 0$ for some γ_i s. Hence if λ is annihilated by some powers of p_i , then $s_i a_i \lambda \in \Lambda_{p_i}/\Lambda'_{p_i}$. Based on the statements above, $\sum_{i=1}^m s_i a_i \lambda = \lambda$, this proves that the S -lattice

$$\lambda \in \Lambda_{p_1}/\Lambda'_{p_1} + \Lambda_{p_2}/\Lambda'_{p_2} + \dots + \Lambda_{p_m}/\Lambda'_{p_m} \quad (3)$$

We suppose $\lambda_i \in \Lambda_{p_i}/\Lambda'_{p_i}$ and $\sum_{i=1}^m \lambda_i = 0$. Then

$$a_i \sum_{j=1}^m \lambda_j = a_i \lambda_i = 0 \quad (4)$$

where (4) follows from the fact that $a_i \lambda_j = 0$ for $i \neq j$. Since a_i is non-zero, λ_i must be zero. Based on the same proof, we can conclude that $\{\lambda_i = 0 | \forall i = 1, 2, \dots, m\}$ provided that $\sum_{i=1}^m \lambda_i = 0$. This suggests that every $\lambda \in \Lambda/\Lambda'$ can be uniquely expressed as the summation of the primary sublattice λ_i , $i = 1, 2, \dots, m$. It implies that there exists a map π :

$$\begin{aligned} & \Lambda_{p_1}/\Lambda'_{p_1} \oplus \Lambda_{p_2}/\Lambda'_{p_2} \oplus \dots \oplus \Lambda_{p_m}/\Lambda'_{p_m} \\ & \longmapsto \Lambda_{p_1}/\Lambda'_{p_1} + \Lambda_{p_2}/\Lambda'_{p_2} + \dots + \Lambda_{p_m}/\Lambda'_{p_m} \end{aligned} \quad (5)$$

defined by

$$\begin{aligned} & \pi(\Lambda_{p_1}/\Lambda'_{p_1} \oplus \Lambda_{p_2}/\Lambda'_{p_2} \oplus \dots \oplus \Lambda_{p_m}/\Lambda'_{p_m}) \\ & = \Lambda_{p_1}/\Lambda'_{p_1} + \Lambda_{p_2}/\Lambda'_{p_2} + \dots + \Lambda_{p_m}/\Lambda'_{p_m} \end{aligned} \quad (6)$$

which is an S -module isomorphism, and also that

$$\Lambda_{p_i}/\Lambda'_{p_i} \cap \sum_{j=1, j \neq i}^m \Lambda_{p_j}/\Lambda'_{p_j} = \mathbf{0} \quad (7)$$

This proves that the sum $\sum_{j=1}^m \Lambda_{p_j}/\Lambda'_{p_j}$ is direct, and hence the map π is an identity map which belongs to automorphism. Theorem 1 is thus proved. ■

Theorem 1 proves that Λ/Λ' can be decomposed into the direct sum of m sublattices $\Lambda_{p_i}/\Lambda'_{p_i}$ (the primary sublattices) which itself forms a new lattice system. Hence Λ/Λ' can be regarded as an m layer

quotient lattice.

Theorem 2: Every primary sublattice $\Lambda_{p_i}/\Lambda'_{p_i}$ is isomorphic to a direct sum of cyclic p_i -torsion modules:

$$\Lambda_{p_i}/\Lambda'_{p_i} \cong S/\langle p_i^{\theta_1} \rangle \oplus S/\langle p_i^{\theta_2} \rangle \oplus \cdots \oplus S/\langle p_i^{\theta_t} \rangle \quad (8)$$

for some integers $1 \leq \theta_1 \leq \theta_2 \leq \cdots \leq \theta_t$ which are uniquely determined by $\Lambda_{p_i}/\Lambda'_{p_i}$.

Proof: Theorem 1 implies that $\Lambda_{p_i}/\Lambda'_{p_i}$ is an $f.g.$ torsion module. Here we write $M_{p_i} = \Lambda_{p_i}/\Lambda'_{p_i}$; let x_1, \dots, x_f be generators for M_{p_i} where f is minimal. This means that M_{p_i}/Sx_1 is generated by $f - 1$ elements, and hence it is a direct sum of $\leq f - 1$ cyclic torsion modules. Thus if $\lambda \in M_{p_i}$ satisfies $p_i^{\theta_t} \lambda = 0$ and $p_i^{\theta_t-1} \lambda \neq 0$, then $M_{p_i} = S\lambda \oplus N \cong (S/\langle p_i^{\theta_t} \rangle)^k \oplus N$, where N is the submodule which is not annihilated by $p_i^{\theta_t}$ although it is annihilated by some other powers of p_i . Given this, we have $M_{p_i}/pM_{p_i} \cong (S/\langle p \rangle)^k \oplus N/pN$ (if $S/\langle p \rangle$ exists), the dimension of the second term, $\dim(N/pN) = \dim(M_{p_i}/pM_{p_i}) - k$. It is clear that the dimension is reduced when the power of p_i increases, until the process ends. This proves that $\Lambda_{p_i}/\Lambda'_{p_i}$ consists of a direct sum of cyclic torsion modules, and hence must be isomorphic to a direct sum of quotient rings over some powers of p_i . This proves the existence of (8).

There exists a chain $0 = p_i^{\theta_t} M_{p_i} \subset \cdots \subset p_i^2 M_{p_i} \subset p_i M_{p_i} \subset M_{p_i}$. Consider that $p_i^{\theta-1} M_{p_i} \cong p_i^{\theta-1} S/p_i^{\theta_1} S \oplus \cdots \oplus p_i^{\theta-1} S/p_i^{\theta_t} S \cong S/\langle p_i^{\theta_t-\theta+1} \rangle \oplus \cdots \oplus S/\langle p_i^{\theta_s-\theta+1} \rangle$. This follows from the third isomorphism theorem and that for those $\theta \geq \theta_i$, $p_i^{\theta}(S/\langle p_i^{\theta_i} \rangle) = 0$. Hence $p_i^{\theta-1} M_{p_i}/p_i^{\theta} M_{p_i} \cong (S/\langle p_i \rangle)^k$ forms a vector space over $S/\langle p_i \rangle$ where k is the number of elementary divisors p_i^{α} with $\alpha \geq \theta$. Thus, $\dim(p_i^{\theta-1} M_{p_i}/p_i^{\theta} M_{p_i})$ is the number of elements in (8) whose $\theta_i \geq \theta$. This proves that the dimension of $p_i^{\theta-1} M_{p_i}/p_i^{\theta} M_{p_i}$ is invariant with M_{p_i} , and the number of summands in a particular form $S/\langle p_i^{\theta_i} \rangle$ is uniquely determined by M_{p_i} . This proves the uniqueness of (8). ■

Theorem 2 implies that the quotient primary S -sublattice system $\Lambda_{p_i}/\Lambda'_{p_i}$ is isomorphic to a cyclic p_i -torsion module. The right-hand side of (8) can be viewed as the message space of $\Lambda_{p_i}/\Lambda'_{p_i}$ which is detailed in Lemma 1.

Lemma 1: There exists a map:

$$\phi_i : \Lambda_{p_i} \mapsto \bigoplus_j S/\langle p_i^{\theta_j} \rangle \quad (9)$$

which is a surjective S -module homomorphism with kernel $\mathcal{K}(\phi_i) = \Lambda'_{p_i}$. To ease the abstract representation, we consider $\Lambda'_{p_i} = \Lambda'$ in the sequel. Thus, $\mathcal{K}(\phi_i) = \Lambda'$ for $i = 1, 2, \dots, m$. If the message space is taken as the canonical decomposition of (8), i.e. $\mathbf{w}^i = \bigoplus_j S/\langle p_i^{\theta_j} \rangle$, there exists a surjective homomorphism

ϕ and also an injective map $\tilde{\phi} : (\mathbf{w}^1, \dots, \mathbf{w}^m) \mapsto \Lambda$ such that

$$\phi(\tilde{\phi}(\mathbf{w}^1 \oplus \dots \oplus \mathbf{w}^m)) = \mathbf{w}^1 \oplus \dots \oplus \mathbf{w}^m \quad (10)$$

Proof: The statement of (9) follows immediately from Theorem 2 and the first isomorphism theorem.

The statement of (10) follows from Theorem 1, Theorem 2 and the first isomorphism theorem. ■

Lemma 2: The generator matrix of the S -sublattice Λ_{p_i} at the i^{th} layer can be expressed in the form of:

$$\mathbf{G}_{\Lambda_{p_i}} = \begin{bmatrix} \text{Diag}(\underbrace{\mathbf{p}_1^{\theta_1} \dots \mathbf{p}_{i-1}^{\theta_{i-1}}, \mathbf{I}_t, \mathbf{p}_{i+1}^{\theta_{i+1}} \dots \mathbf{p}_m^{\theta_m}}_k) & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_{n-k} \end{bmatrix} \mathbf{G}_{\Lambda} \quad (11)$$

and

$$\phi_i(\mathbf{w} \mathbf{G}_{\Lambda_{p_i}}) = (w^{i,1} + \langle p_i^{\theta_1} \rangle, \dots, w^{i,t} + \langle p_i^{\theta_t} \rangle) \quad (12)$$

where $w^{i,t} \in S/\langle p_i^{\theta_t} \rangle$ and $\mathbf{w} \in \mathbf{w}^1 \oplus \dots \oplus \mathbf{w}^m$. \mathbf{G}_{Λ} is the generator matrix of the fine lattice Λ , $\mathbf{p}_j^{\theta_j}$, $j = 1, 2, \dots, m$ is a vector, with all elements being the same elementary divisor $p_j^{\theta_j}$ over S , and $t = \dim(\Lambda_{p_i}/\Lambda')$.

Proof: Every matrix over a PID must have a Smith normal form (SNF) with unique invariant factors up to multiplication by units. This complies with the structure theorem of modules over PID in invariant factor form. Hence there exists an *equivalent* SNF matrix \mathbf{M}_{SNF} such that $\mathbf{M}_{\text{SNF}} \mathbf{G}_{\Lambda_{p_i}}$ is the generator matrix of the lattice $\tilde{\Lambda}'$ which is isomorphic to the kernel $\mathcal{K}(\phi_i) = \Lambda'$. Based on the theorems mentioned above and the fact that the invariant factors are uniquely determined, the invariant factors in \mathbf{M}_{SNF} must be some powers of p_i which naturally satisfies the divisibility relations, and we claim that, now $\tilde{\Lambda}' = \Lambda'$. The statement of (12) follows from Lemma 1. ■

Lemma 2 shows a way to produce the quotient S -sublattice of each layer defined in Theorem 1. Λ_{p_i}/Λ' forms an independent lattice system, and the direct sum of all Λ_{p_i}/Λ' , $i = 1, 2, \dots, m$ is equal to Λ/Λ' .

B. Construction of multilevel lattice network coding

Based on the Theorems developed in section III-A, we show in this subsection the detailed description of the MLNC scheme, and a way of multilevel network decoding (named layered integer forcing), which provides an efficient way of decoding the linear combination of the multi-source messages with greatly reduced complexity.

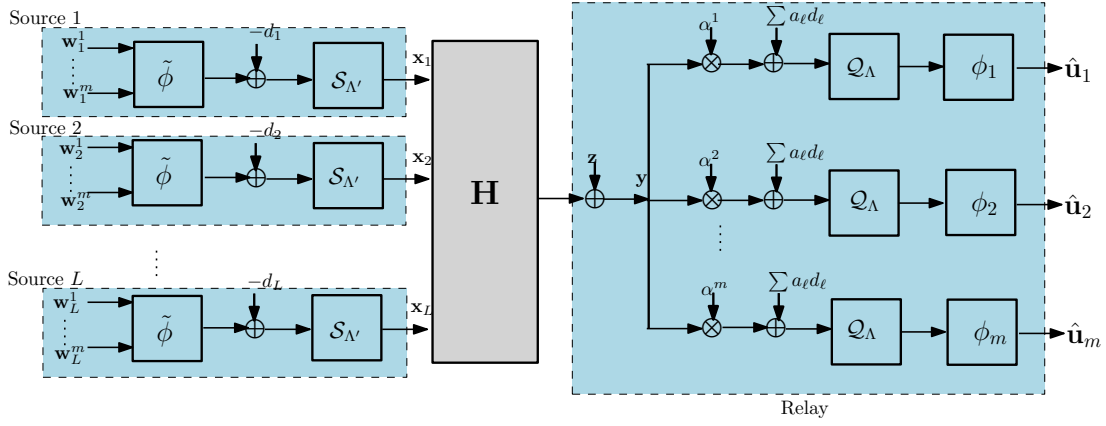


Fig. 1. System diagram of the multilevel lattice network coding and multistage decoding. The right-hand side of \mathbf{H} represents the decoding for a single relay.

Traditional Approach: Theorem 1, Theorem 2 and Lemma 1 imply that the message space with large cardinality may be expressed as a set of smaller message spaces over the hybrid finite field and finite chain ring. Fig. 1 depicts a multilevel lattice network coding architecture, with L sources and a single relay. The encoder \mathcal{E}_ℓ at the ℓ^{th} source maps the original message $\mathbf{w}_\ell = \mathbf{w}_\ell^1 \oplus \cdots \oplus \mathbf{w}_\ell^m$ to a fine lattice point Λ (assuming n -dimension) via the injective map $\tilde{\phi}$ defined in Lemma 1. Then we add a dither $\mathbf{d}_\ell \in \mathbb{C}^n$ which is uniformly distributed over the fundamental Voronoi region $\mathcal{V}_{\Lambda'}$ of Λ' . The dithered lattices pass through a nested shaping operator in order to restrain the power consumption. This operation is performed via the sublattice quantization:

$$\lambda'_\ell = \mathcal{Q}_{\Lambda'}(\tilde{\phi}(\mathbf{w}_\ell^1 \oplus \cdots \oplus \mathbf{w}_\ell^m) + \mathbf{d}_\ell) \quad (13)$$

where $\lambda'_\ell \in \Lambda'$, and $\mathcal{Q}_{\Lambda'}(\cdot) : \mathbb{C}^n \mapsto \Lambda'$ is a coarse lattice quantizer. The output of the ℓ^{th} source is given by:

$$\begin{aligned} \mathbf{x}_\ell &= \mathcal{E}_\ell(\mathbf{w}_\ell^1 \oplus \cdots \oplus \mathbf{w}_\ell^m) \\ &= \tilde{\phi}(\mathbf{w}_\ell^1 \oplus \cdots \oplus \mathbf{w}_\ell^m) + \mathbf{d}_\ell - \lambda'_\ell \end{aligned} \quad (14)$$

Note that \mathbf{x}_ℓ is uniformly distributed over $\mathcal{V}_{\Lambda'}$ due to the effect of the dither. The average power of the transmitted signal \mathbf{x}_ℓ is given by:

$$P = \frac{1}{n \text{Vol}(\mathcal{V}_{\Lambda'})} \int_{\mathcal{V}_{\Lambda'}} \|\mathbf{x}_\ell\|^2 d\mathbf{x}_\ell \quad (15)$$

which is the second moment per dimension of \mathbf{x}_ℓ over $\mathcal{V}_{\Lambda'}$. The message space at each source consists of a direct sum of m small message spaces (assuming there are m levels) over different finite fields or

chain rings. The encoder \mathcal{E}_ℓ constructs a one-to-one relation between the message space and the coset system Λ/Λ' .

At the relay, given the received signals \mathbf{y} and an S -integer vector $\tilde{\mathbf{a}} = [\tilde{a}_1, \tilde{a}_2, \dots, \tilde{a}_L]^T \in S^L$, the decoder aims at computing a new lattice point which is regarded as an S -linear combination of transmitted lattice points from all sources. The homomorphism designed for the coset system will be used for decoding the lattice point to a linear combination of the original messages. We assume in this paper that the fading coefficients $\mathbf{h} = [h_1, h_2, \dots, h_L]$, and dithers are perfectly known at the relay. The decoder can be described, generally, by:

$$\mathcal{D} : (\mathbb{C}^n, \mathbb{C}^L, S^L, \mathbb{C}, \mathbb{C}^{n \times L}) \mapsto W \quad (16)$$

Thus, the output of $\mathcal{D}(\mathbf{y}|\mathbf{h}, \tilde{\mathbf{a}}, \alpha, \mathbf{d})$ is the estimates of the linear combination of the original messages of each source. Here α is a scaling factor [5] which maximises the computation rate. Note that the aforementioned decoder (16) may vary according to the specific problem. There may be additional information available to the decoder, and the decoder may also have extra outputs. However, basically the core idea for the decoding remains the same. Based on the quotient lattice Λ/Λ' , we have:

$$\begin{aligned} \hat{\mathbf{u}} &= \mathcal{D}(\mathbf{y}|\mathbf{h}, \mathbf{a}, \alpha, \mathbf{d}) \\ &\stackrel{(a)}{=} \phi \left(\mathcal{Q}_\Lambda \left(\alpha \mathbf{y} - \sum_{\ell=1}^L \tilde{a}_\ell \mathbf{d}_\ell \right) \right) \end{aligned} \quad (17)$$

$$\stackrel{(b)}{=} \phi \left(\mathcal{Q}_\Lambda \left(\sum_{\ell=1}^L \tilde{a}_\ell \left(\tilde{\phi}(\mathbf{w}_\ell) - \lambda'_\ell \right) + \mathbf{n}_{\text{eff}} \right) \right) \quad (18)$$

$$\stackrel{(c)}{=} \phi \left(\sum_{\ell=1}^L \tilde{a}_\ell \tilde{\phi}(\mathbf{w}_\ell) + \mathcal{Q}_\Lambda(\mathbf{n}_{\text{eff}}) \right) \quad (19)$$

$$\stackrel{(d)}{=} \bigoplus_{\ell=1}^L a_\ell \mathbf{w}_\ell \boxplus \phi(\mathcal{Q}_\Lambda(\mathbf{n}_{\text{eff}})) \quad (20)$$

where (a) follows from the fact that we expect to quantize a set of scaled received signals which are subtracted from the corresponding dithers. (b) follows from the manipulation of:

$$\alpha \mathbf{y} = \sum_{\ell=1}^L \tilde{a}_\ell \mathbf{x}_\ell + \sum_{\ell=1}^L \tilde{a}_\ell \mathbf{d}_\ell + \overbrace{\sum_{\ell=1}^L (\alpha h_\ell - \tilde{a}_\ell) \mathbf{x}_\ell}^{\mathbf{n}_{\text{eff}}} + \alpha \mathbf{z} \quad (21)$$

(c) follows from the definition of the lattice quantizer, and (d) follows from the properties of a surjective

module homomorphism, and also Lemma 1. Note that here $\phi(\tilde{a}_\ell) = a_\ell \in \mathbf{w}^1 \oplus \cdots \oplus \mathbf{w}^m$.

Equations (17) - (20) reveal the decoding operations for the traditional lattice-based PNC. We are able to decode a linear combination of messages $\bigoplus_{\ell=1}^L a_\ell \mathbf{w}_\ell$ over all sources without errors provided that $\phi(\mathcal{Q}_\Lambda(\mathbf{n}_{\text{eff}})) = 0$. Thus, the successful decoding is guaranteed iff the effective noise is quantized to the kernel of ϕ , $\mathcal{K}(\phi)$.

The problems left unsolved are: 1. how to exploit rich ring features in order to make it practically applicable in lattice-based network coding. 2. when the cardinality (the coset representatives) of Λ/Λ' is large, the complexity of the lattice quantizer becomes unmanageable, which restricts the application of LNC. What is the practical lattice network decoding approach that could greatly relieve the decoding load in LNC. We study a new decoding solution which is specifically designed in terms of MLNC, and which relaxes the two problems mentioned.

Layered Integer Forcing: The breakthrough of MLNC (based on Theorems and Lemmas in section III-A) is that

- The original message space over Λ/Λ' can be decomposed into a direct sum of m smaller message spaces in terms of Λ_{p_i}/Λ' , $i = 1, 2, \dots, m$.
- The relay can decode each layer independently; thus the decoder tries to infer and forward a linear combination of messages of each layer *separately* over the message subspace defined in Theorem 2.

Let us recall the traditional decoding operations explained in (17) - (20). If we are only concerned with the linear combination of a particular layer, the quantization of the effective noise need not necessarily be the kernel of ϕ . There must exist other lattice points in Λ/Λ' such that the homomorphism of these points does not interfere with the linear combination of that layer following the aforementioned theorems.

Theorem 3: There exists a quotient S -lattice Λ/Λ'_i with generator matrices \mathbf{G}_Λ for Λ , and $\mathbf{G}_{\Lambda'_i}$ for Λ'_i , which satisfies:

$$\mathbf{G}_{\Lambda'_i} = \begin{bmatrix} \text{Diag}(\underbrace{\mathbf{I}, p_i^{\theta_1}, \dots, p_i^{\theta_t}, \mathbf{I}}_k) & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_{n-k} \end{bmatrix} \mathbf{G}_\Lambda \quad (22)$$

and there is a surjective S -module homomorphism φ_i :

$$\varphi_i : \Lambda \longmapsto S/\langle p_i^{\theta_1} \rangle \oplus S/\langle p_i^{\theta_2} \rangle \oplus \cdots \oplus S/\langle p_i^{\theta_t} \rangle \quad (23)$$

whose kernel $\mathcal{K}(\varphi_i) = \Lambda'_i$. The quotient S -lattice Λ/Λ'_i is isomorphic to the direct sum of cyclic modules:

$$\Lambda/\Lambda'_i \cong S/\langle p_i^{\theta_1} \rangle \oplus S/\langle p_i^{\theta_2} \rangle \oplus \cdots \oplus S/\langle p_i^{\theta_t} \rangle \quad (24)$$

Proof: By applying the equivalent SNF explained in the proof of Lemma 2, we can prove (22) in similar way. Now we begin the proof of (23). The sublattice Λ'_i can be written as:

$$\Lambda'_i = \{\mathbf{w}\mathbf{G}_\Lambda : \mathbf{w}^i \in \langle p_i^{\theta_1} \rangle \oplus \cdots \oplus \langle p_i^{\theta_t} \rangle\}$$

in terms of the generator matrix for Λ'_i in (22). It is clear that:

$$\varphi_i(\mathbf{w}\mathbf{G}_\Lambda) = 0 \quad \text{iff} \quad \mathbf{w}^i \in \langle p_i^{\theta_1} \rangle \oplus \cdots \oplus \langle p_i^{\theta_t} \rangle$$

and hence, the kernel of φ_i , $\mathcal{K}(\varphi_i)$ must be Λ'_i . It is also obvious from (23) that φ_i is indeed surjective and S -linear. The proof of (24) follows immediately from the first isomorphism theorem. ■

Note that although both Λ_{p_i}/Λ' and Λ/Λ'_i are isomorphic to $S/\langle p_i^{\theta_1} \rangle \oplus S/\langle p_i^{\theta_2} \rangle \oplus \cdots \oplus S/\langle p_i^{\theta_t} \rangle$, they belong to different coset systems. Λ_{p_i}/Λ' is related to the construction of lattices that have multilevel structure, whereas Λ/Λ'_i is related to the decoding issues, i.e. LIF.

Theorem 3 defines a new sublattice Λ'_i which plays a key role in decoding MLNC, as it is the kernel of the quotient S -lattice that possesses a surjective homomorphism φ_i for the i^{th} layer. Hence it is possible to decode an S -linear combination of fine lattice points to an S -linear combination of the original messages of the i^{th} layer. This is explained in Lemma 3.

Lemma 3: Given the embedding injective map $\tilde{\phi} : (\mathbf{w}^1, \dots, \mathbf{w}^m) \mapsto \Lambda$, there exists a surjective S -module homomorphism φ_i , $i = 1, 2, \dots, m$, defined in (23), satisfying:

$$\varphi_i\left(\tilde{\phi}(\mathbf{w}^1 \oplus \cdots \oplus \mathbf{w}^m)\right) = \begin{cases} \mathbf{w}^i, & \mathbf{w}^i \notin \langle p_i^{\theta_1} \rangle \oplus \cdots \oplus \langle p_i^{\theta_t} \rangle \\ 0, & \mathbf{w}^i \in \langle p_i^{\theta_1} \rangle \oplus \cdots \oplus \langle p_i^{\theta_t} \rangle \end{cases} \quad (25)$$

Proof: The injective mapping $\tilde{\phi}$ is an inverse operation of the homomorphism ϕ defined in terms of the quotient S -lattice Λ/Λ' , which maps the messages into a lattice point Λ , as explained in Lemma 1. Following the second statement of Theorem 3, the S -module homomorphism φ_i of the i^{th} layer indeed maps the lattice point Λ to the message subspace. When $\mathbf{w}^i \in \langle p_i^{\theta_1} \rangle \oplus \cdots \oplus \langle p_i^{\theta_t} \rangle$, $\tilde{\phi}(\mathbf{w}^1 \oplus \cdots \oplus \mathbf{w}^m)$ maps to the lattice point Λ'_i which is the kernel of φ_i . Hence, according to (22), the linear labelling of the new coset system in Λ/Λ'_i coincides with the labelling of the i^{th} layer of $\tilde{\phi}$. This proves Lemma 3. ■

Based on Lemma 3, it is now possible to decode the linear combination of the messages of each layer separately and independently. Assuming the messages at the i^{th} layer is of interest, the relay computes:

$$\hat{\mathbf{u}}^i = \mathcal{D}^i(\mathbf{y}|\mathbf{h}, \mathbf{a}^i, \alpha^i, \mathbf{d}) \quad (26)$$

$$= \varphi_i \left(\mathcal{Q}_\Lambda \left(\alpha^i \mathbf{y} - \sum_{\ell=1}^L \tilde{a}_\ell^i \mathbf{d}_\ell \right) \right) \quad (27)$$

where

$$\mathcal{D}^i : (\mathbb{C}^n, \mathbb{C}^L, S^L, \mathbb{C}, \mathbb{C}^{n \times L}) \mapsto W^i \quad (28)$$

and $\alpha^i \in \mathbb{C}$ and \mathbf{a}^i are scaling parameter and S -integer coefficients of the i^{th} layer, respectively, which are determined by some optimisation criterion in terms of the quotient S -lattice Λ/Λ'_i .

Theorem 3 and Lemma 3 lay the foundation of the layered integer forcing. The linear combination of $\hat{\mathbf{u}}^i$ can be recovered in terms of LIF by:

$$\begin{aligned} \hat{\mathbf{u}}^i &\stackrel{(d)}{=} \varphi_i \left(\mathcal{Q}_\Lambda \left(\sum_{\ell=1}^L \tilde{a}_\ell^i \left(\tilde{\phi}(\mathbf{w}_\ell^1 \oplus \cdots \oplus \mathbf{w}_\ell^m) - \lambda'_\ell \right) + \mathbf{n}_{\text{eff}} \right) \right) \\ &\stackrel{(e)}{=} \varphi_i \left(\sum_{\ell=1}^L \tilde{a}_\ell^i \tilde{\phi}(\mathbf{w}_\ell^1 \oplus \cdots \oplus \mathbf{w}_\ell^m) - \lambda'_\ell - \lambda'_{i,\ell} + \mathcal{Q}_\Lambda(\mathbf{n}_{\text{eff}}) \right) \\ &\stackrel{(f)}{=} \varphi_i \left(\sum_{\ell=1}^L \tilde{a}_\ell^i \tilde{\phi}(\mathbf{w}_\ell^1 \oplus \cdots \oplus \mathbf{w}_\ell^m) \right) \boxplus \varphi_i \left(\mathcal{Q}_\Lambda(\mathbf{n}_{\text{eff}}) \right) \\ &\stackrel{(g)}{=} \bigoplus_{\ell=1}^L a_\ell^i \mathbf{w}_\ell^i \boxplus \varphi_i \left(\mathcal{Q}_\Lambda(\mathbf{n}_{\text{eff}}) \right) \end{aligned} \quad (29)$$

where (d) follows from (14) and basic arithmetic manipulations; (e) follows from the definition of the lattice quantizer \mathcal{Q}_Λ , and also the S -linear combination of the lattice points is restricted in $\mathcal{V}_{\Lambda'_i}$; (f) follows from the property of a surjective S -module homomorphism, and also the fact that $\lambda' \subseteq \lambda'_i$ and $\mathcal{K}(\varphi_i) = \lambda'_i$. (g) follows from Lemma 3, and note that $\varphi_i(\tilde{a}_\ell^i) = a_\ell^i \in W^i$.

Lemma 4: The linear combination of the messages at the i^{th} layer $\hat{\mathbf{u}}^i = \bigoplus_{\ell=1}^L a_\ell^i \mathbf{w}_\ell^i$ can be recovered iff $\mathcal{Q}_\Lambda(\mathbf{n}_{\text{eff}}) \in \Lambda'_i$. Thus, $\Pr(\hat{\mathbf{u}}^i \neq \mathbf{u}^i) = \Pr(\mathcal{Q}_\Lambda(\mathbf{n}_{\text{eff}}) \notin \Lambda'_i)$.

Proof: Following (29), it is clear that $\hat{\mathbf{u}}^i = \bigoplus_{\ell=1}^L a_\ell^i \mathbf{w}_\ell^i$ can be decoded correctly iff $\varphi_i \left(\mathcal{Q}_\Lambda(\mathbf{n}_{\text{eff}}) \right) = 0$. According to Theorem 3, the kernel of φ_i , $\mathcal{K}(\varphi_i) = \Lambda'_i$; thus the quantization of the effective noise $\mathcal{Q}_\Lambda(\mathbf{n}_{\text{eff}}) \in \Lambda'_i$. This proves Lemma 4. ■

Lemma 4 reveals that the lattice Λ'_i defined in Theorem 3 plays a key role in decoding the messages of the i^{th} layer.

The message space of the traditional C&F scheme is determined by the size of the lattice partition. Hence, to increase the network throughput, the sublattice Λ' needs to be more sparse in order to allow the messages to be over a larger field or commutative ring (LNC). In this case, the decoding complexity is normally unaffordable.

One example is associated with a group of lattice codes directly designed in the Euclidean space, e.g. complex low density lattice codes (CLDLC). It has prohibitive computational complexity when the cardinality of the quotient lattice is too large, since the decoding metrics are continuous functions (a mixture of multiple probability density functions), and the periodic extension that occurs at the variable nodes [4] runs over a large S -integer set, which seriously increases the overall computational costs over the iterative parametric belief propagation decoding, even if the Gaussian mixture reduction algorithm is employed.

The S -lattices can also be constructed through the existing channel codes based on some lattice construction approaches (e.g. construction A, D). However, the decoding complexity of the channel codes over a large algebraic field increases rapidly, e.g. a small increase of the memory for convolutional codes gives rise to an exponential increase in the number of trellis states, making the codes eventually undecodable. When the cardinality of the quotient lattices become larger, the decoding complexity for convolutional codes with even small memory is unmanageable, but the performance is still very poor.

MLNC together with LIF provides a realistic solution to this problem. Being supported by the Theorems and Lemmas in sections III-A and III-B, the quotient S -lattice having large cardinality can be decomposed into some primary quotient S -sublattices which have smaller cardinalities. Each primary quotient sublattice forms a layer, and determines the message subspace over this layer. With the aid of the lattices Λ'_i , we can perform multilevel lattice decoding at the relay, where the linear combination of the messages of all sources at each layer can be independently recovered over the message subspace. In this case, the overall computational loads are greatly relaxed.

LNC [6] shows the possibility of ring-based linear network coding, extending the traditional linear network coding defined over the finite field to a more general notion. Furthermore, MLNC leads to a practically feasible encoding and decoding design approach for lattice network coding over commutative rings, thus, with greatly reduced decoding complexity. MLNC inherently gives an appealing solution for this since now we are able to construct multiple layers based on the decomposition theory mentioned

above, with each layer operating over a finite field or chain ring in a new coset system. Note that the elements in a finite chain ring can be uniquely represented by $\nu + 1$ elements over a fixed residue field where ν is the nilpotency index of this finite chain ring. We will introduce this in the subsequent sections.

C. Achievable Rates and Probability of Error

As discussed in section III-B, the message of the i^{th} layer corresponds to the decomposed quotient S -sublattice Λ_{p_i}/Λ' , which should be decoded separately at each layer, based on a new S -lattice partition Λ/Λ'_i . Suppose that each layer is given an S -integer coefficient vector $\mathbf{a}^i \in S^L$, and $\mathbf{A} = [\mathbf{a}^1 | \mathbf{a}^2 | \dots | \mathbf{a}^m] \in S^{L \times m}$, we can obtain the achievable rate following Nazer and Gastpar's method, under the assumption of that S is Gaussian integers $\mathbb{Z}[i]$

Theorem 4: Given channel fading vector $\mathbf{h} \in \mathbb{C}^L$, non-zeros S -integer coefficient matrix $\mathbf{A} \notin \{0\}$, and the message subspace $W^i = \left(\mathbb{Z}[i]/\langle p_i \rangle\right)^k$, the probability of decoding error $\Pr(\hat{\mathbf{u}}^i \neq \mathbf{u}^i | \mathbf{h}, \mathbf{A})$ can be arbitrarily small if the overall message rate \mathcal{R} satisfies:

$$\mathcal{R} < \mathcal{R}(\mathbf{h}, \mathbf{A}) = \sum_i^m \log_2 \left(\left(\|\mathbf{a}^i\|^2 - \frac{P^i |\mathbf{h}^\dagger \mathbf{a}^i|^2}{1 + P^i \|\mathbf{h}\|^2} \right)^{-1} \right) \quad (30)$$

for sufficiently large lattice dimension n and prime factor p_i . $P^{(i)}$ is defined by

$$P^{(i)} = \frac{1}{n \text{Vol}(\mathcal{V}_{\Lambda/\Lambda'_i})} \int_{\mathcal{V}_{\Lambda/\Lambda'_i}} \|\mathbf{x}_\ell\|^2 d\mathbf{x}_\ell \quad (31)$$

Proof: Suppose there are m layers, we can construct a quotient $\mathbb{Z}[i]$ -lattice Λ/Λ'_i which is isomorphic to the message subspace W^i . The computation rate of each layer follows from Nazer and Gastpar's method in [5]. Since each layer is decoded independently, the sum of computation rate of all layers is the overall achievable rate. ■

Recall Lemma 4, the error probability of decoding a linear combination \mathbf{u} in terms of \mathbf{a}^i for the i^{th} level is equal to the probability of $\Pr(\mathcal{Q}_\Lambda(\mathbf{n}_{\text{eff}}) \notin \Lambda'_i)$. The union bound of the error probability for MLNC is given by:

Theorem 5: Given $\mathbf{h} \in \mathbb{C}^L$, non-zeros S -integer coefficient matrix $\mathbf{A} \notin \{0\}$, and the optimal scaling factor α_{opt} , the union bound of the error probability in decoding the linear combinations of all levels in

MLNC is given by:

$$\begin{aligned}
& \Pr \left(\hat{\mathbf{u}} \neq \mathbf{u} | \mathbf{h}, \mathbf{A}, \alpha_{\text{opt}} \right) \\
&= \mathbf{E}_{p(\mathcal{Z})} \left[\Pr(\hat{\mathbf{u}}^i \neq \mathbf{u}^i | \mathbf{h}, \mathbf{A}, \alpha_{\text{opt}}) \right] \\
&\lesssim \mathbf{E}_{p(\mathcal{Z})} \left[\mathcal{N}(\Lambda/\Lambda'_i) \exp \left(\frac{-d^2(\Lambda/\Lambda'_i)}{4(N_0|\alpha_{\text{opt}}|^2 + P^i||\alpha_{\text{opt}}\mathbf{h} - \mathbf{a}^i||^2)} \right) \right] \tag{32}
\end{aligned}$$

where \mathcal{Z} is a random variable with its outcomes taking on $\{r = \frac{\dim(\mathbf{u}^i)}{\dim(\mathbf{u})} | i = 1, 2, \dots, m\}$.

Proof: At the i^{th} layer, the decoding operates over the lattice partition of $\Lambda/\Lambda'_i = \{\Lambda \setminus \Lambda'_i\} \cup \{\mathbf{0}\}$. $d(\Lambda/\Lambda'_i)$ is the minimum inter-coset distance of the lattice partition Λ/Λ'_i defined by

$$d(\Lambda/\Lambda'_i) = \min ||\boldsymbol{\vartheta}_1 - \boldsymbol{\vartheta}_2||^2, \boldsymbol{\vartheta}_1, \boldsymbol{\vartheta}_2 \in \Lambda/\Lambda'_i, \boldsymbol{\vartheta}_1 \neq \boldsymbol{\vartheta}_2$$

We denote $\mathcal{N}(\Lambda/\Lambda'_i)$ as the number of $d(\Lambda/\Lambda'_i)$ in the i^{th} layer coset system. Following the steps in [6], we can prove that the probability error of effective noise quantization is bounded by the probability of effective noise which is not within the Voronoi region \mathcal{V}_0 :

$$\Pr \left(\mathcal{Q}_\Lambda(\mathbf{n}_{\text{eff}}) \notin \Lambda'_i | \mathbf{h}, \mathbf{a}^i, \alpha_{\text{opt}} \right) \leq \Pr \left(\mathbf{n}_{\text{eff}} \notin \mathcal{V}_0^i | \mathbf{h}, \mathbf{a}^i, \alpha_{\text{opt}} \right)$$

with

$$\mathcal{V}_0^i = \{\boldsymbol{\vartheta} \in \mathbb{C}^n : ||\boldsymbol{\vartheta} - \mathbf{0}||^2 \leq ||\boldsymbol{\vartheta} - \lambda||^2, \forall \lambda \in \Lambda \setminus \Lambda'_i\}$$

The probability of $\Pr(\mathbf{n}_{\text{eff}} \notin \mathcal{V}_0^i | \mathbf{h}, \mathbf{a}^i, \alpha_{\text{opt}})$ is upper bounded by the term within the bracket of (32). The proof closely follows from the method given in [6], based on the Chernoff inequality, the moment generating function of a complex Gaussian random vector, and hypercube Voronoi region Λ'_i . We refer to [6] for the detailed proof, and also [7] for the proof under Eisenstein integers. Since each layer decodes the linear combination independently, the average error probability is the expectation of $\Pr(\hat{\mathbf{u}}^i \neq \mathbf{u}^i | \mathbf{h}, \mathbf{A}, \alpha_{\text{opt}})$ over the probability function $p(\mathcal{Z})$. According to Lemma 3, we know that the probability $\Pr(\hat{\mathbf{u}}^i \neq \mathbf{u}^i | \mathbf{h}, \mathbf{A}, \alpha_{\text{opt}}) \leq \Pr(\mathbf{n}_{\text{eff}} \notin \mathcal{V}_0^i | \mathbf{h}, \mathbf{a}^i, \alpha_{\text{opt}})$; this gives (32). \blacksquare

One way to design the homomorphism of Λ/Λ'_i at the i^{th} layer is implied in Theorem 5. Thus, $\mathcal{N}(\Lambda/\Lambda'_i)$ should be minimised and $d(\Lambda/\Lambda'_i)$ is maximized such that the probability of error is as small as possible

at the i^{th} layer. It is clear that MLNC has good flexibility in the design of the homomorphism, which determines the achievable rate at some levels.

IV. ELEMENTARY DIVISOR CONSTRUCTION

In this section, we study a new lattice construction approach, based on the Theorems and Lemmas developed in section III-A.

Lemma 5: Let Λ and Λ' be S -lattices and S -sublattices, $\Lambda' \subseteq \Lambda$, $|\Lambda : \Lambda'| < \infty$ such that Λ/Λ' has a nonzero annihilator ϖ which can be uniquely factorised into distinct powers of primes in S , $\varpi = \mathcal{U}(S)p_1^{\gamma_1}p_2^{\gamma_2}\cdots p_m^{\gamma_m}$. Then Λ/Λ' is the direct sum of a finite number of quotient sublattices, $\Lambda_{p_i}/\Lambda' = \{\lambda \in \Lambda/\Lambda' : p_i^{\gamma_i}\lambda = 0\}$, $i = 1, 2, \dots, m$, and given by,

$$\Lambda/\Lambda' = \Lambda_{p_1}/\Lambda' \oplus \Lambda_{p_2}/\Lambda' \oplus \cdots \oplus \Lambda_{p_m}/\Lambda' \quad (33)$$

Proof: Lemma 5 is a special case of Theorem 1 where the annihilator of Λ/Λ' is a single S -integer. Therefore Λ/Λ' must be the direct sum of some new quotient S -lattices. The annihilator of the Λ_{p_i}/Λ' is precisely $p_i^{\gamma_i}$. ■

A. Elementary Divisor Construction

We outline a possible lattice construction solution based on Lemma 5 and the statements in section III-A.

Elementary Divisor Construction (EDC): Let p_1, p_2, \dots, p_m be some distinct primes in a PID S , and $\varpi = \mathcal{U}(S)p_1^{\gamma_1}p_2^{\gamma_2}\cdots p_m^{\gamma_m}$ is a unique factorisation, $\gamma_i \geq 1$. Let $\mathcal{C}^1, \mathcal{C}^2, \dots, \mathcal{C}^m$ be m $[n, k_i]$ linear codes over $S/\langle p_1^{\gamma_1} \rangle, S/\langle p_2^{\gamma_2} \rangle, \dots, S/\langle p_m^{\gamma_m} \rangle$, respectively. The elementary divisor construction lattice is defined by:

$$\Lambda \triangleq \{\lambda \in S^n : \tilde{\sigma}(\lambda) \in \mathcal{C}^1 \oplus \mathcal{C}^2 \oplus \cdots \oplus \mathcal{C}^m\} \quad (34)$$

and the sublattice is:

$$\Lambda' \triangleq \{\varpi\lambda : \lambda \in S^n\}$$

where $\tilde{\sigma} : S^n \mapsto (S/\langle p_1^{\gamma_1} \rangle)^n \oplus (S/\langle p_2^{\gamma_2} \rangle)^n \oplus \cdots \oplus (S/\langle p_m^{\gamma_m} \rangle)^n$ is a natural map obtained by extending the ring homomorphism $\sigma : S \mapsto S/\langle p_1^{\gamma_1} \rangle \times S/\langle p_2^{\gamma_2} \rangle \times \cdots \times S/\langle p_m^{\gamma_m} \rangle$ to multiple dimensions. Apparently

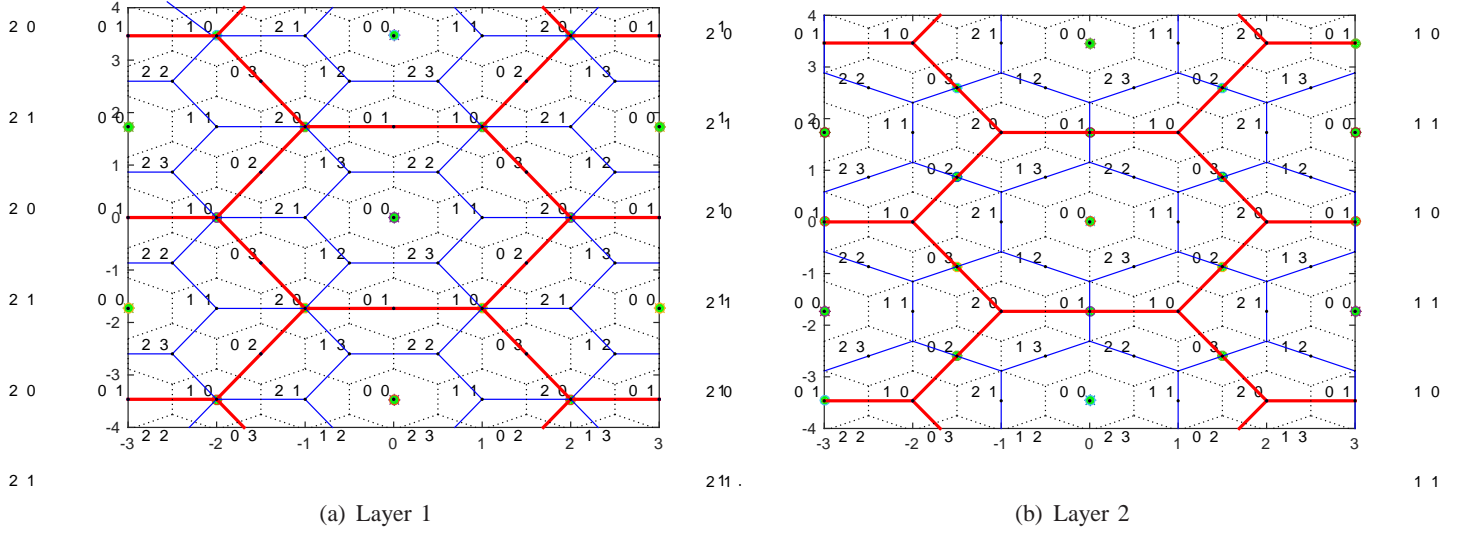


Fig. 2. Layer structure of a 2-layer EDC lattice. The green points and blue lines represent the primary sublattices and Voronoi region of $\mathcal{V}_{\Lambda'_i}$ for the corresponding layers, respectively. Dotted lines represent the Voronoi region of the fine lattice.

$\Lambda' \subseteq \Lambda$. The message space under EDC is

$$W = (S/\langle p_1^{\gamma_1} \rangle)^{k_1} \oplus \cdots \oplus (S/\langle p_m^{\gamma_m} \rangle)^{k_m} \quad (35)$$

where k_i is the message length of the i^{th} layer which sums up to $k = \sum_{j=1}^m k_j$.

The elementary divisor construction is a straightforward extension of Lemma 5, which defines a class of lattices constructed by m linear codes, with each operating over either a finite field or a finite chain ring. Hence the quotient Λ/Λ' must consist of m primary sublattices Λ_{p_i}/Λ' , with each constructed by the i^{th} linear code. The primary sublattices Λ_{p_i} of the i^{th} layer is defined by:

$$\Lambda_{p_i} \triangleq \{\lambda_{p_i} \in \delta_i S : \tilde{\sigma}_i(\lambda_{p_i}) \in C^i\} \quad (36)$$

where $\tilde{\sigma}_i$ is a natural map:

$$\tilde{\sigma}_i : (\delta_i S)^n \mapsto (\delta_i S/p_i^{\gamma_i} \delta_i S)^n \cong (S/\langle p_i^{\gamma_i} \rangle)^{k_i} \quad (37)$$

obtained by extending the ring homomorphism $\sigma_i : \delta_i S \mapsto \delta_i S/\langle p_i^{\gamma_i} \delta_i S \rangle$ to multiple dimensions. The scaling factor $\delta_i = \frac{\varpi}{p_i^{\gamma_i}}$ can be proved in terms of the proof in Theorem 1.

We consider three scenarios based on different algebraic fields which the linear codes may belong to.

Scenario 1: Assume that the primary sublattice at each layer is constructed by a linear code over a finite field, thus, $\gamma_1 = \gamma_2 = \cdots = \gamma_m = 1$. Then, $C^i \in (\delta_i S/\langle p_i \delta_i \rangle)^n$. Since the coarse lattice Λ' is generated by a single element ϖ , Λ/Λ' forms a cyclic torsion module which allows us to produce the

generator matrix of the i^{th} layer lattice Λ_{p_i} . It will have a form described in Lemma 2, given by:

$$\mathbf{G}_{\Lambda_{p_i}} = \begin{bmatrix} \text{Diag} \left(\mathbf{p}_1^{(k_1)} \cdots \mathbf{p}_{i-1}^{(k_{i-1})}, \mathbf{I}_{k_i}, \mathbf{p}_{i+1}^{(k_{i+1})} \cdots \mathbf{p}_m^{(k_m)} \right) & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_{mn-k} \end{bmatrix} \mathbf{G} \quad (38)$$

where $\mathbf{p}_i^{(k_i)}$ is a length- k_i vector with each element p_i . $\mathbf{G}_{\Lambda_{p_i}}$ in (38) gives the generator matrix for the i^{th} layer lattices, when the message input

$$\mathbf{w} = [\mathbf{w}^1, \mathbf{w}^2, \dots, \mathbf{w}^m, \underbrace{\tilde{d}_1 \cdots \tilde{d}_m}_{mn-k}] \quad (39)$$

where $\mathbf{w}^i \in (\delta_i S / \langle p_i \delta_i \rangle)^{k_i}$, $\tilde{d}_i \in S^{n-k_i}$.

Since EDC lattices are constructed by some linear codes, the matrix \mathbf{G} must include the generator matrix of each linear code \mathcal{C}^i . Let $\tilde{\sigma}_i([\mathbf{I}_{k_i} \quad \mathbf{B}_{k_i \times (n-k_i)}^i])$ be a generator matrix for a linear code \mathcal{C}^i (without loss of generality, we consider that the linear code is systematic in this case.), then \mathbf{G} is an $n \times n$ matrix defined below,

$$\mathbf{G} = \begin{bmatrix} \mathbf{I}_{k_1} & \mathbf{B}_{k_1 \times (n-k_1)}^1 \\ \mathbf{I}_{k_2} & \mathbf{B}_{k_2 \times (n-k_2)}^2 \\ \vdots & \vdots \\ \mathbf{I}_{k_m} & \mathbf{B}_{k_m \times (n-k_m)}^m \\ \mathbf{0} & \varpi \mathbf{I}_{n-k_1} \\ \vdots & \vdots \\ \mathbf{0} & \varpi \mathbf{I}_{n-k_m} \end{bmatrix} \quad (40)$$

Equation (40) follows from Lemma 5 and part of the proof of Theorem 1 (i.e. (6)). The generator matrix of the coarse lattice Λ' is therefore given by,

$$\mathbf{G}_{\Lambda'} = \begin{bmatrix} \text{Diag} \left(\mathbf{I}_{\sum_{j=1}^{i-1} k_j}, \mathbf{p}_i^{(k_i)}, \mathbf{I}_{\sum_{j=i+1}^m k_j} \right) & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_{mn-k} \end{bmatrix} \mathbf{G}_{\Lambda_{p_i}} \quad (41)$$

It can be easily observed that these generator matrices are consistent with the Theorems and Lemmas proposed in section III. Note that the generator matrix for linear code \mathcal{C}^i is $\tilde{\sigma}_i([\mathbf{I}_{k_i} \quad \mathbf{B}_{k_i \times (n-k_i)}^i])$ where $\tilde{\sigma}_i$ is defined in (37). Theorem 3 establishes the theoretic fundamental for low-complexity lattice decoding (i.e. LIF) of MLNC, and states that there exists a surjective S -module homomorphism φ_i which satisfies

$$\mathbf{G}_{\text{FCR}}^i = \left[\begin{array}{ccccc|c} \mathbf{I}_{k'_{i,0}} & Z_{0,1}^i & Z_{0,2}^i & \cdots & Z_{0,\gamma_i-1}^i & Z_{0,\gamma_i}^i \\ 0 & p_i \mathbf{I}_{k'_{i,1}} & p_i Z_{1,2}^i & \cdots & p_i Z_{1,\gamma_i-1}^i & p_i Z_{1,\gamma_i}^i \\ 0 & 0 & p_i^2 \mathbf{I}_{k'_{i,2}} & \cdots & p_i^2 Z_{2,\gamma_i-1}^i & p_i^2 Z_{2,\gamma_i}^i \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & p_i^{\gamma_i-1} \mathbf{I}_{k'_{i,\gamma_i-1}} & p_i^{\gamma_i-1} Z_{\gamma_i-1,\gamma_i}^i \end{array} \right] = \left[\mathcal{I}_{p_i^{\gamma_i}}^* \mid \mathcal{B}_{k'_{i,n-k'_i}} \right] \quad (43)$$

Lemma 3, with kernel $\mathcal{K}(\varphi_i) = \Lambda'_i$, which plays a key role in decoding the i^{th} layer linearly combined messages. Its generator matrix has a form:

$$\mathbf{G}_{\Lambda'_i} = \left[\begin{array}{cc} \text{Diag}(\mathbf{I}, \underbrace{\mathbf{p}_i^{(k_i)}}_k, \mathbf{I}) & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_{mn-k} \end{array} \right] \mathbf{G} \quad (42)$$

We can easily verify $\Lambda/\Lambda'_i \cong (S/\langle p_i \rangle)^{k_i}$ in terms of these generator matrices.

Scenario 2: When $\forall i = 1, 2, \dots, m, \gamma_i \neq 1$, the primary sublattice Λ_{p_i} at each layer is constructed by a linear code over a finite chain ring $T = \delta_i S / \langle p_i^{\gamma_i} \delta_i \rangle$ [11]. A finite chain ring is a finite local principal ideal ring, and the most remarkable characteristic of a finite chain ring is that its every ideal (including $\langle 0 \rangle$) is generated by the maximal ideal, which can be linearly ordered by inclusion, and hence, forms a chain. The finite chain ring T has a unique maximal ideal and hence the resultant residue field is $Q = \delta_i S / \langle p_i \delta_i \rangle$ with size $q = |\delta_i S / \langle p_i \delta_i \rangle|$. The chain length of the ideals is indeed the nil-potency index of p_i which is, in this case γ_i . We refer to T a (q, γ_i) chain ring.

At the i^{th} layer, the generator matrix $\mathbf{G}_{\text{FCR}}^i$ of a linear code over T has a standard form given in (43), where $\mathbf{I}_{k'_{i,t}}$ denotes an identity matrix with dimension $k'_{i,t}$,¹ $i = 1, 2, \dots, m$ and $t = 0, 1, \dots, \gamma_i - 1$. Hence $\mathbf{G}_{\text{FCR}}^i$ has a dimension $k'_i \times n$ where $k'_i = \sum_{t=0}^{\gamma_i-1} k'_{i,t}$. Here $Z_{t,l}$, $l = t+1, 2, \dots, \gamma_i$, denotes a $k'_{i,t} \times k'_{i,l+1}$ ($k'_{i,\gamma_i} = n - k'_i$) matrix which is unique modulo $p_i^{\gamma_i-t}$ [12]. In (43), $\mathcal{I}_{p_i^{\gamma_i}}^*$ is an upper triangular matrix with dimension $k'_i \times k'_i$, and $\mathcal{B}_{k'_{i,n-k'_i}}$ has a dimension of $k'_i \times (n - k'_i)$. Note that the codeword is row spanned by $\mathbf{G}_{\text{FCR}}^i$ and all rows of $\mathbf{G}_{\text{FCR}}^i$ are linearly independent.

To study the message space of the linear codes over the finite chain ring, we first examine the kernel of the generator matrix $\mathbf{G}_{\text{FCR}}^i$. This is equivalent to finding the null space for the encoder $\mathcal{E}^i : \mathbf{w}^i \mapsto \mathcal{C}^i$, where $\mathcal{E}^i(\mathbf{w}^i) \triangleq \mathbf{w}^i \mathbf{G}_{\text{FCR}}^i$ and $\mathbf{w}^i = [\mathbf{w}_{k'_{i,0}}, \mathbf{w}_{k'_{i,1}}, \dots, \mathbf{w}_{k'_{i,\gamma_i-1}}]$. Here \mathbf{w}^i is grouped into blocks of size $\mathbf{w}_{k'_{i,t}}$ which corresponds to the row blocks defined in (43). In order to obtain the all-zero codeword $\mathcal{C}^i = \mathbf{0}$, we solve the homogeneous system $\mathbf{w}^i \mathbf{G}_{\text{FCR}}^i = \mathbf{0}$, which gives $\mathbf{w}_{k'_{i,t}} \in p_i^{\gamma_i-t} T^{k'_{i,t}}$, $t = 0, 1, \dots, \gamma_i - 1$.

¹Here, the index i used in $k'_{i,t}$ is the indicator of layer.

This result is based on the fact that if $d \in T^n$, then $p_i^t d = 0 \implies d \in p_i^{\gamma_i - t} T^n$. The null space of the encoder \mathcal{E}^i is therefore:

$$\mathbf{w}' = [p_i^{\gamma_i} T^{k'_{i,0}}, \dots, p_i T^{k'_{i,\gamma_i-1}}] \quad (44)$$

According to the first isomorphism theorem, the codeword \mathcal{C}^i is isomorphic to a direct summation:

$$\begin{aligned} \mathcal{C}^i &\cong (T/p_i^{\gamma_i} T)^{k'_{i,0}} \oplus (T/p_i^{\gamma_i-1} T)^{k'_{i,1}} \oplus \dots \oplus (T/p_i T)^{k'_{i,\gamma_i-1}} \\ &\cong (\delta_i S / \langle p_i^{\gamma_i} \delta_i \rangle)^{k'_{i,0}} \oplus (\delta_i S / \langle p_i^{\gamma_i-1} \delta_i \rangle)^{k'_{i,1}} \oplus \dots \oplus (\delta_i S / \langle p_i \delta_i \rangle)^{k'_{i,\gamma_i-1}} \end{aligned} \quad (45)$$

The right-hand side of (45) denotes the message space \mathbf{W}^i of the linear code over the finite chain ring T in terms of the generator matrix $\mathbf{G}_{\text{FCR}}^i$. Note that each component in the direct sum of (45) forms another module or vector space, and the size of the t^{th} component is $q^{(\gamma_i - t)k'_{i,t}}$. This leads to the overall message size $|\mathcal{C}| = q^{\sum_{t=0}^{\gamma_i-1} (\gamma_i - t)k'_{i,t}}$. Of course, we can obtain this result directly from the kernel of $\mathbf{G}_{\text{FCR}}^i$, thus, $|\mathcal{C}| = \prod_{t=0}^{\gamma_i-1} (p_i^t T)^{k'_{i,t}}$ which gives the same result.

Let $\tilde{\mathbf{p}}_i^{\gamma_i}$ be a length- k'_i vector:

$$\tilde{\mathbf{p}}_i^{\gamma_i} \triangleq [\mathbf{p}_{i,(k'_{i,0})}^{\gamma_i}, \mathbf{p}_{i,(k'_{i,1})}^{\gamma_i-1}, \dots, \mathbf{p}_{i,(k'_{i,\gamma_i-1})}]$$

where $\mathbf{p}_{i,(k'_{i,0})}^{\gamma_i}$ denotes a length- $k'_{i,0}$ vector, with each component being $p_i^{\gamma_i}$. Note that $\tilde{\mathbf{p}}_i^{\gamma_i}$ is closely related to (44). Following Lemma 2, the generator matrix of the primary sublattice Λ_{p_i} of the i^{th} layer in this scenario has a form:

$$\mathbf{G}_{\Lambda_{p_i}} = \begin{bmatrix} \text{Diag}(\tilde{\mathbf{p}}_1^{\gamma_1} \dots \tilde{\mathbf{p}}_{i-1}^{\gamma_{i-1}}, \mathbf{I}_{k'_i}, \tilde{\mathbf{p}}_{i+1}^{\gamma_{i+1}} \dots \tilde{\mathbf{p}}_m^{\gamma_m}) & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_{mn-k'} \end{bmatrix} \mathbf{G} \quad (46)$$

where $k' = \sum_{i=1}^m k'_i$. The EDC lattices in this scenario are constructed by some linear codes over different finite chain rings, and the matrix \mathbf{G} must be associated with the generator matrix of each linear code \mathcal{C}^i over the finite chain ring. Let $\tilde{\sigma}_i(\mathbf{d} \cdot [\tilde{\mathcal{Z}}_{p_i}^* \quad \tilde{\mathcal{B}}_{k'_i, n-k'_i}])$ be the codeword of $\mathcal{C}^i = \mathbf{w}^i \mathbf{G}_{\text{FCR}}^i$ over the finite

chain ring T , $\mathbf{d} \in \delta_i S^{k'_i}$. Then, \mathbf{G} in (46) is an $mn \times n$ matrix defined below:

$$\mathbf{G} = \begin{bmatrix} \tilde{\mathcal{I}}_{p_1}^* & \tilde{\mathcal{B}}_{k'_1, n-k'_1} \\ \tilde{\mathcal{I}}_{p_2}^* & \tilde{\mathcal{B}}_{k'_2, n-k'_2} \\ \vdots & \vdots \\ \tilde{\mathcal{I}}_{p_m}^* & \tilde{\mathcal{B}}_{k'_m, n-k'_m} \\ \mathbf{0} & \varpi \mathbf{I}_{n-k'_1} \\ \vdots & \vdots \\ \mathbf{0} & \varpi \mathbf{I}_{n-k'_m} \end{bmatrix} \quad (47)$$

Hence, we are able to construct Λ_{p_i} and hence the EDC lattice Λ for this scenario based on the generator matrices presented above. Note that message space of each layer follows from (45), and $k'_{i,t}$ should be selected such that

$$\gamma_i k_i = \sum_{t=0}^{\gamma_i-1} (\gamma_i - t) k'_{i,t} \quad (48)$$

in order to guarantee the consistency to the message size of the i^{th} layer EDC lattices defined in (35). It is easy to prove that there exists $k'_{i,t} \in \mathbb{Z}^+$, $\forall t = 0, 1, \dots, \gamma_i - 1$, satisfying (48).

The generator matrix of the coarse lattice Λ' is given by,

$$\mathbf{G}_{\Lambda'} = \begin{bmatrix} \text{Diag} \left(\mathbf{I}_{\sum_{j=1}^{i-1} k'_j}, \tilde{\mathbf{p}}_i^{\gamma_i}, \mathbf{I}_{\sum_{j=i+1}^m k'_j} \right) & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_{mn-k} \end{bmatrix} \mathbf{G}_{\Lambda_{p_i}} \quad (49)$$

Following (49), it is obvious that $\Lambda/\Lambda' \cong \mathbf{W}^1 \oplus \dots \oplus \mathbf{W}^m$. The generator matrix for Λ'_i has a form:

$$\mathbf{G}_{\Lambda'_i} = \begin{bmatrix} \text{Diag} \left(\mathbf{I}_{\sum_{j=1}^{i-1} k'_j}, \tilde{\mathbf{p}}_i^{\gamma_i}, \mathbf{I}_{\sum_{j=i+1}^m k'_j} \right) & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_{mn-k} \end{bmatrix} \mathbf{G} \quad (50)$$

which will be used for LIF detection.

Every ideal of T is generated by the maximal ideal, which forms a chain with chain length γ_i . Hence the residue field Q plays an important role in producing the linear codes over T . We now consider a

matrix in the form of:

$$\mathbf{G}_D^i = \text{Diag} \left(\mathbf{p}_{i,(k'_{i,0})}^0, \dots, \mathbf{p}_{i,(k'_{i,\gamma_i-1})}^{\gamma_i-1} \right) \begin{bmatrix} \mathbf{g}_{k'_{i,0}}^i \\ \mathbf{g}_{k'_{i,1}}^i \\ \vdots \\ \mathbf{g}_{k'_{i,\gamma_i-1}}^i \end{bmatrix} \quad (51)$$

where $\mathbf{g}_{k'_{i,t}}^i \in Q_{k'_{i,t} \times n}^*$, and $Q_{k'_{i,t} \times n}^*$ is a $k'_{i,t} \times n$ matrix with each entry over the coset representative of the residue field $Q = \delta_i S / \langle p_i \delta_i \rangle$. Each row of \mathbf{G}_D^i must satisfy the condition that none of its rows are linear combinations of the other rows. The message space of \mathbf{G}_D^i could be partitioned into $\gamma_i - 1$ levels. We first define the vector $\beta_{k'_{i,t}}^{(j)} = [\beta_1^{(j)}, \beta_2^{(j)}, \dots, \beta_{k'_{i,t}}^{(j)}]$, when $t = 0$, where $j = 0, 1, \dots, \gamma_i - 1$, is the level indicator, and $\beta_{k'_{i,t}}^{(j)} = [\beta_{k'_{i,t-1}+1}^{(j)}, \beta_{k'_{i,t-1}+2}^{(j)}, \dots, \beta_{k'_{i,t}}^{(j)}]$ when $t = 1, 2, \dots, \gamma_i - 1$. Accurately $\beta_{k'_{i,t}}^{(j)}$ represents a length- $k'_{i,t}$ segment of the j^{th} level message over the vector space $Q^{k'_{i,t}}$. The full message space of the j^{th} level is given by,

$$\beta^{(j)} = [p_i^j \beta_{k'_{i,0}}^{(j)}, p_i^{j-1} \beta_{k'_{i,1}}^{(j)}, p_i^{j-2} \beta_{k'_{i,2}}^{(j)}, \underbrace{\mathbf{0} \dots \mathbf{0}}_{k'_i - \sum_{t=0}^j k'_{i,t}}] \quad (52)$$

where the powers of p_i can not be negative integers. Hence the message space of \mathbf{G}_D^i is $W^i = \beta^{(0)} + \beta^{(1)} + \dots + \beta^{(\gamma_i-1)}$. The codewords \mathcal{C}^i can be produced by

$$\begin{aligned} \mathcal{C}^i &= W^i \mathbf{G}_D^i = \left(\beta^{(0)} + \beta^{(1)} + \dots + \beta^{(\gamma_i-1)} \right) \mathbf{G}_D^i \\ &= \mathbf{c}_0^i + \mathbf{c}_1^i p_i + \dots + \mathbf{c}_{\gamma_i-1}^i p_i^{\gamma_i-1} \end{aligned} \quad (53)$$

Since none of the rows of \mathbf{G}_D^i are linear combinations of the other rows, \mathbf{c}_t^i is therefore row spanned by

$$\mathbf{g}_{\mathbf{c}_t^i}^i = \left[\mathbf{g}_{k'_{i,0}}^i; \mathbf{g}_{k'_{i,1}}^i; \dots; \mathbf{g}_{k'_{i,t}}^i \right] \quad (54)$$

It is obvious that \mathbf{c}_t^i , $t = 0, 1, \dots, \gamma_i - 1$ forms a set of nested codes $\mathbf{c}_0^i \subseteq \mathbf{c}_1^i \subseteq \dots \subseteq \mathbf{c}_{\gamma_i-1}^i$ over Q^* . Following the Q -adic decomposition theorem of finite chain ring [12][11], we assert that the codeword \mathcal{C}^i in (53) generated by \mathbf{G}_D^i is indeed over T .

In terms of (51) and (52), the message space corresponding to $\mathbf{g}_{k'_{i,t}}^i$ should be written as:

$$W_t^i = \sum_{j=t}^{\gamma_i-1} p_i^{j-t} \beta_{k'_{i,t}}^{(j)} \quad (55)$$

this complies with the Q -adic decomposition and leads to the result that the message space corresponding to $\mathbf{g}_{k'_{i,t}}^i$ is $(T/\langle p_i^{\gamma_i-t} \rangle)^{k'_{i,t}}$. This implies that the right-hand side of (45) is precisely the message space of \mathbf{G}_D^i . Mathematically the primary sublattices Λ_{p_i} can also be represented in the form below:

$$\Lambda_{p_i} = \bigcup \left\{ \underbrace{\sum_{j=0}^{\gamma_i-1} \sum_{\ell=1}^{\mathcal{K}_j^i} p_i^j \beta_{\ell}^{(j)} \mathbf{g}_{\ell}^i}_{(52)} + p_i^{\gamma_i} S^n | \mathbf{g}_{\ell}^i \in Q_{1 \times n} \right\} \quad (56)$$

where $\mathcal{K}_j^i = k'_{i,0} + \dots + k'_{i,j}$. It is interesting to see that (56) has the same structure as complex construction D. Now we conclude that the primary S -sublattices constructed by a linear code over a finite chain ring subsumes construction D.

Based on this result, we may now construct EDC lattices for this scenario using a set of nested linear codes over a finite field. Let $\mathbf{g}_{(n-k'_i)}^i \in Q_{n-k'_i \times n}^*$ be an $(n - k'_i) \times n$ matrix, then the \mathbf{G} matrix is:

$$\mathbf{G} = \left[\mathbf{G}_D^{1T}, \dots, \mathbf{G}_D^{mT}, \varpi \mathbf{g}_{(n-k'_i)}^{1T}, \dots, \varpi \mathbf{g}_{(n-k'_i)}^{mT} \right]^T \quad (57)$$

Scenario 3: This corresponds to a hybrid case of scenario 1 and 2, and we give the following summaries:

- 1) $m = 1, \gamma_1 = 1$, then the EDC lattice in (34) is a complex construction A lattice which is indecomposable.
- 2) $m = 1, \gamma_1 > 1, \gamma_1 \in \mathbb{Z}^+$ then the EDC lattice in (34) is a complex construction D lattice which is indecomposable.
- 3) $m > 1, m, \gamma_i \in \mathbb{Z}^+, i = 1, 2, \dots, m$, then the EDC lattice in (34) is decomposable, and consists of some sublattices constructed by either construction A or D.

Note that in 3), a new class of lattices over S is generated by a number of linear codes over either finite field or chain ring, which generalises the scenario 1 and 2. Scenario 3 suggests that the design of EDC lattices is very flexible, and we also give more detailed discussion about why EDC lattices are good at low-complexity decoding and throughput improvement for PNC in the next sections.

B. Nominal coding gain and Kissing number

In this section, we study the nominal coding gain and kissing number of the EDC lattices for all three scenarios. The definition such as the minimum-norm coset leaders and minimum Euclidean weight of the codeword follows from [6].

Scenario 1: We first study the nominal coding gain and kissing number of the i^{th} layer primary sublattices in this scenario. Following (36) and (37), we know that \mathcal{C}^i is a linear code of length n over $\delta_i S/p_i \delta_i S$. Thus, $\mathbf{c}^i = (c_1^i + \langle \varpi \rangle, \dots, c_n^i + \langle \varpi \rangle) \in \mathcal{C}^i$. We denote $\omega^{(i)}(\mathbf{c}^i)$ the Euclidean weight of a codeword \mathbf{c}^i in \mathcal{C}^i , and $\omega_{\min}^{(i)}(\mathcal{C}^i)$ the minimum Euclidean weight of non-zero codewords in \mathcal{C}^i . Let ϑ be a scaling factor depending on which PID is used, and $N(\omega_{\min}^{(i)}(\mathcal{C}^i))$ be the number of codewords in \mathcal{C}^i with the minimum Euclidean weight $\omega_{\min}^{(i)}(\mathcal{C}^i)$.

Proposition 1: Let \mathcal{C}^i be a linear code over $\delta_i S/p_i \delta_i S$, and Λ_{p_i}/Λ' the primary quotient lattice system of the i^{th} layer constructed by \mathcal{C}^i , $\Lambda_{p_i} \supseteq \Lambda'$, then the nominal coding gain is given by:

$$\varrho(\Lambda_{p_i}/\Lambda') = \frac{\omega_{\min}^{(i)}(\mathcal{C}^i)}{\vartheta |p_i|^{2(1-\frac{k_i}{n})} |\delta_i|^2} \quad (58)$$

and the kissing number is:

$$K(\Lambda_{p_i}/\Lambda') = \begin{cases} N(\omega_{\min}^{(i)}(\mathcal{C}^i)) \left(\frac{\mathcal{N}_{\mathcal{U}(S)}}{|p_i|^2 - 1} \right)^{\frac{\omega_{\min}^{(i)}(\mathcal{C}^i)}{|\delta_i|^2}}, & |p_i|^2 - 1 \leq \mathcal{N}_{\mathcal{U}(S)} \\ N(\omega_{\min}^{(i)}(\mathcal{C}^i)), & \text{Otherwise} \end{cases} \quad (59)$$

Proof: See Appendix D. ■

Here $\mathcal{N}_{\mathcal{U}(S)}$ represents the number of units in S .

It is of interest to study the nominal coding gain and kissing number of Λ/Λ' in terms of the m linear codes \mathcal{C}^i . Following the proof of Theorem 1, and the descriptions in section IV-A, $\tilde{\mathbf{c}} = \mathbf{c}^1 + \mathbf{c}^2 + \dots + \mathbf{c}^m$, $\tilde{\mathbf{c}} \in \tilde{\mathcal{C}}$ and $\tilde{\mathcal{C}} \in (S/\langle \varpi \rangle)^n$. Thus, the nominal coding gain of EDC lattices is determined by the m linear codes \mathcal{C}^i over $\delta_i S/p_i \delta_i S$, $i = 1, 2, \dots, m$.

Proposition 2: Let $\mathcal{C}^1, \dots, \mathcal{C}^m$ be m linear codes over $\delta_i S/p_i \delta_i S$, $i = 1, 2, \dots, m$, respectively. Let $\tilde{\mathbf{c}} = \mathbf{c}^1 + \mathbf{c}^2 + \dots + \mathbf{c}^m$, $\tilde{\mathbf{c}} \in \tilde{\mathcal{C}}$ and $\mathbf{c}^i \in \mathcal{C}^i$. The nominal coding gain of the EDC lattices Λ/Λ' in scenario 1 is given by

$$\varrho(\Lambda/\Lambda') = \frac{\omega_{\min}(\tilde{\mathcal{C}}) \prod_{\ell=2}^m |p_j|^{\frac{2(k_\ell - k_1)}{n}}}{\vartheta |p_1|^{2(1-\frac{k_1}{n})} |\delta_1|^2} \quad (60)$$

where $k_1 \leq k_2 \leq \dots \leq k_m$.

Proof: See Appendix D. ■

Scenario 2: This corresponds to the case where $\gamma_i > 1$, $\gamma_i \in \mathbb{Z}$ for $i = 1, 2, \dots, m$. The primary sublattice of the i^{th} layer can be constructed by a linear code \mathcal{C}^i over a finite chain ring $\delta_i S / \langle \varpi \rangle$, where $\delta_i = \frac{\varpi}{p_i^{\gamma_i}}$. This follows immediately from (36) and (37). Here, we are more concerned with the nominal coding gain and kissing number when the i^{th} primary sublattice is constructed by a set of nested linear codes over the residue field Q , since the linear code over a finite field is easier to generate. Let $\mathcal{C}^{i,0} \subseteq \dots \subseteq \mathcal{C}^{i,\gamma_i-1}$ be nested linear codes of length- n over Q , where $\mathcal{C}^{i,t}$ is an $[n, \sum_{\ell=0}^t k'_{i,\ell}]$ linear code for the t^{th} nested code at the i^{th} layer, and we denote $\omega_{\min}^{(i,t)}(\mathcal{C}^{i,t})$ the minimum Euclidean weight of non-zero codewords in $\mathcal{C}^{i,t}$. We have:

Proposition 3: Let $\mathcal{C}^{i,0} \subseteq \dots \subseteq \mathcal{C}^{i,\gamma_i-1}$ be γ_i nested linear codes of length- n over Q , and Λ_{p_i}/Λ' be the primary quotient lattice of the i^{th} layer constructed from $\mathcal{C}^{i,t}$, $t = 0, 1, \dots, \gamma_i - 1$, then the nominal coding gain of the i^{th} layer is lower bounded by

$$\varrho(\Lambda_{p_i}/\Lambda') \geq \frac{|p_i|^{\frac{2}{n} \sum_{t=0}^{\gamma_i-1} (\gamma_i-t)k'_{i,t}} \min_{0 \leq t \leq \gamma_i-1} \{|p_i|^{2t} \omega_{\min}^{(i,t)}(\mathcal{C}^{i,t})\}}{\vartheta|\varpi|^2} \quad (61)$$

and the kissing number is upper bounded by:

$$K(\Lambda_{p_i}/\Lambda') \leq \begin{cases} \sum_{t=0}^{\gamma_i-1} N_t(\omega_{\min}^{(i,t)}(\mathcal{C}^{i,t})) \left(\frac{\mathcal{N}_{\mathcal{U}(S)}}{|p_i|^2-1} \right)^{\frac{\omega_{\min}^{(i,t)}(\mathcal{C}^{i,t})}{|\delta_i|^2}}, & |p_i|^2 - 1 \leq \mathcal{N}_{\mathcal{U}(S)} \\ \sum_{t=0}^{\gamma_i-1} N_t(\omega_{\min}^{(i,t)}(\mathcal{C}^{i,t})), & \text{Otherwise} \end{cases} \quad (62)$$

Proof: See Appendix E. ■

It is of interest to study the nominal coding gain of Λ/Λ' in this scenario. If each primary sublattice is constructed via a set of nested linear codes over a finite field $Q = \delta_i S / \langle p_i \delta_i \rangle$ for the i^{th} layer, the nominal coding gain $\varrho(\Lambda/\Lambda')$ will be related to overall $\sum_{i=1}^m \gamma_i$ linear codes since there are γ_i nested linear codes for each i . Let $\tilde{\mathcal{C}}$ be a composite code such that $\tilde{\mathbf{c}} = \mathbf{c}^1 + \dots + \mathbf{c}^m$ where $\mathbf{c}^i = \mathbf{c}^{i,0} + p_i \mathbf{c}^{i,1} + \dots + p_i^{\gamma_i-1} \mathbf{c}^{i,\gamma_i-1}$. Hence $\mathcal{C}^i \in \delta_i S / \langle \varpi \rangle$ and $\tilde{\mathcal{C}} \in S / \langle \varpi \rangle$. We denote $\omega_{\min}(\tilde{\mathcal{C}})$ the minimum Euclidean weight of non-zero codewords in $\tilde{\mathcal{C}}$, then:

Proposition 4: Let $\mathcal{C}^{i,0} \subseteq \dots \subseteq \mathcal{C}^{i,\gamma_i-1}$ be γ_i nested linear codes of length- n over Q , and let $\tilde{\mathcal{C}}$ be a composite code such that $\tilde{\mathbf{c}} = \mathbf{c}^1 + \dots + \mathbf{c}^m$ where $\mathbf{c}^i = \mathbf{c}^{i,0} + p_i \mathbf{c}^{i,1} + \dots + p_i^{\gamma_i-1} \mathbf{c}^{i,\gamma_i-1}$. The nominal

coding gain for Λ/Λ' in scenario 2 is given by:

$$\begin{aligned}\varrho(\Lambda/\Lambda') &= \frac{\omega_{\min}(\tilde{\mathcal{C}})}{(V(\mathcal{V}(\Lambda)))^{\frac{1}{n}}} \\ &= \frac{\omega_{\min}(\tilde{\mathcal{C}}) \prod_{i=1}^m |p_i|^{2 \sum_{t=0}^{\gamma_i-1} (\gamma_i - t) \frac{k'_{i,t}}{n}}}{\vartheta |\varpi|^2}\end{aligned}\quad (63)$$

Proof: See Appendix E. ■

Scenario 3: As explained in the preceding section, in this case, $\gamma_i \geq 1$, $\gamma_i \in \mathbb{Z}$, and hence the EDC lattice consists of a number of primary sublattices which can be constructed by linear codes over either finite field or finite chain ring. The nominal coding gain and kissing number of the primary sublattices in each case have been derived in Proposition 1 and 3. We are more interested in the nominal coding gain of Λ/Λ' in this scenario. Again, we consider the primary sublattices of scenario 2 is constructed over a set of nested linear codes. Let $\tilde{\mathcal{C}}$ be a composite code such that $\tilde{\mathbf{c}} = \mathbf{c}^1 + \dots + \mathbf{c}^m$ where

$$\mathbf{c}^i = \begin{cases} \mathbf{c}^i, & \mathbf{c}^i \in \delta_i S / p_i \delta_i S, & \gamma_i = 1 \\ \mathbf{c}^{i,0} + p_i \mathbf{c}^{i,1} + \dots + p_i^{\gamma_i-1} \mathbf{c}^{i,\gamma_i-1}, & \mathbf{c}^{i,t} \in Q, & \gamma_i > 1 \end{cases}$$

We can easily prove that $\varrho(\Lambda/\Lambda')$ has similar form as (63) if we set $k'_{i,0} = k_i$ for $\gamma_i = 1$.

V. ITERATIVE DETECTION OF EDC AND THE EXIT CHART ANALYSIS

In this section we present an iteration-aided multistage decoding approach specifically designed for EDC, which provides a feasible way of improving the performance of decoding the linear combinations, and also of increasing the overall rate with low decoding-complexity. In the remainder of the paper, we consider S to be a ring of Eisenstein integers $\mathbb{Z}[\omega]$. However, the results can be readily extended to other PIDs.

Section IV clearly reveals the possible encoding structure for EDC. Recalling the definition for EDC, we know that the map $\tilde{\sigma} : S^n \mapsto (S/\langle p_1^{\gamma_1} \rangle)^n \oplus (S/\langle p_2^{\gamma_2} \rangle)^n \oplus \dots \oplus (S/\langle p_m^{\gamma_m} \rangle)^n$ is a natural projection of a surjective ring homomorphism $\sigma : S \mapsto S/\langle p_1^{\gamma_1} \rangle \times S/\langle p_2^{\gamma_2} \rangle \times \dots \times S/\langle p_m^{\gamma_m} \rangle \longleftrightarrow \mathbb{F}_{\tilde{p}_1} \times \dots \times \mathbb{F}_{\tilde{p}_m}$ by applying it element-wise [13] ($\gamma_i = 1, \forall i = 1, 2, \dots, m$). Note that in this case, σ is actually an $f.g.$ abelian group homomorphism. It is easy to see that each level $S/\langle p_i \rangle$ is coded by an $[n, k_i]$ linear code \mathcal{C}^i over $\mathbb{F}_{\tilde{p}_i}$ (a finite field or finite chain ring determined by \tilde{p}_i).

The Type-1 Eisenstein primes are those primes $p \in \mathbb{Z}$ which either have a form $6j+5$, $j \in \mathbb{Z}$, or $p = 2$. Their associates are also categorised as Type-1. The Type-2 Eisenstein primes have the form $\tau = a + b\omega$, $a, b \neq 0$ where the norm $\mathcal{N}(\tau)$ of τ is a prime $p \in \mathbb{Z}$ satisfying $p \equiv 1 \pmod{6}$. Note that if $\tau = a + b\omega$ is

a prime in $\mathbb{Z}[\omega]$, $\tau' = b + a\omega$ is also a prime in $\mathbb{Z}[\omega]$. Hence τ and τ' are distinct primes categorised as Type-2. Together with the Type-3 Eisenstein primes, $\varpi \in \mathbb{Z}[\omega]$ can be uniquely decomposed into:

$$\varpi = \mathcal{U}(\mathbb{Z}[\omega])2^e \prod_{i=1}^{\kappa_1} \tau_i^{\mu_i} \prod_{j=1}^{\kappa_2} \tau_j'^{\eta_j} \prod_{k=1}^{\kappa_3} p_k^{\beta_k} \cdot (1 + 2\omega)^s \quad (64)$$

Accordingly, $\mathbb{Z}[\omega]/\langle 2 \rangle \cong \mathbb{F}_{2^2}$, $\mathbb{Z}[\omega]/\langle \tau \rangle \cong \mathbb{F}_{\mathcal{N}(\tau)}$, $\mathbb{Z}[\omega]/\langle p \rangle \cong \mathbb{F}_{p^2}$, $\mathbb{Z}[\omega]/\langle 1 + 2\omega \rangle \cong \mathbb{F}_3$.

A. Soft Detector for EDC

Section III gives a general decoding method LIF for MLNC, based on the optimised scaling factor α , S -integer coefficient vectors $\tilde{\mathbf{a}}_i$, and a good EDC lattice quantizer, e.g. a Viterbi decoder with modified metrics (see Appendix C). Thus, when EDC is employed in MLNC, LIF is also feasible. In this section, we explore another detection approach designed specifically for the EDC-based MLNC (which follows from the structure of the EDC lattices). Especially an iterative detector is developed, which exploits the multilevel structure gain of EDC by using multistage decoding.

First, we consider the non-iterative multistage decoding. The detector tries to decode the linear function of each level stage-by-stage, with the aid of the *a priori* information from the preceding layers. The detection structure is similar to the point-to-point multilevel codes, e.g. [14, 15] whereas here the *a priori* information is the soft estimation. We develop a layered soft detector (LSD) which calculates the posteriori L-vector (a vector of Log-likelihood ratio) for each layer with the aid of the multiple *a priori* L-vectors. The detailed derivation is given in Appendix A.

The LSD decodes the linear function of each layer over the corresponding non-binary finite field, and hence the *a priori* information of each layer is no longer a scalar value. We define the *a priori* information \mathbf{A}^i to be a vector-based random variable with realization:

$$\mathbf{a}^i = \left[\log \left(\frac{\Pr(\xi|V^i = v_1^i)}{\Pr(\xi|V^i = 0)} \right) \cdots \log \left(\frac{\Pr(\xi|V^i = v_{\tilde{p}_i-1}^i)}{\Pr(\xi|V^i = 0)} \right) \right] \quad (65)$$

where V^i denotes the possible linear combinations at the i^{th} level, which is a uniformly distributed random variable whose k^{th} realization is $v_k^i \in \mathbb{F}_{\tilde{p}_i}$, $k = 1, 2, \dots, \tilde{p}_i - 1$. $\Pr(\xi|V^i = v_k^i)$ is the probability of the *a priori* channel outputs $\Xi = \xi$ given the event $V^i = v_k^i$. Assume that $w_j^i \in \mathbb{F}_{\tilde{p}_i}$, $i = 1, 2, \dots, m$, $j = 1, 2, \dots, L$ to be the message of the i^{th} level and the j^{th} source, the linear function is defined by $f^i(w_1^i, \dots, w_L^i) = \bigoplus_{\ell=1}^L a_\ell^i w_\ell^i$ over $\mathbb{F}_{\tilde{p}_i}$. Note that the integer coefficient a_ℓ^i can be determined either by the lattice reduction approach as introduced in [6, 16] over the i^{th} quotient lattice Λ/Λ'_i as defined in Theorem 3, or by the maximum mutual information criterion as described later.

In the multistage iterative decoding, the proposed LSD outputs the extrinsic L-vector \mathbf{e}^i for the i^{th} level, based on the *a priori* L-vector $\mathbf{a}^j, j \in \{1, \dots, m\}, j \neq i$. Assume that there is a two level EDC and the decoding proceeds from layer 1 (which is regarded as the 1st stage decoding) to layer 2 (the 2nd stage decoding). The extrinsic outputs of layer 1 feed into layer 2 to assist the 2nd stage decoding. With the aid of the *a priori* L-value, layer 2 estimates and forwards the extrinsic information (which serves as the *a priori* information of layer 1) to layer 1. The process is repeated and all layers are activated in turn for the second and subsequent iterations. We refer to this approach as the iterative MSD (IMSD) scheme for MLNC. The detection process is similar to iterative decoding of multilevel codes, e.g. [17] whereas the nature of the detection is different. As the iteration proceeds, each layer will produce more reliable extrinsic L-vector \mathbf{e}^i which also serves as the *a priori* information of the soft-in soft-out non-binary decoder for the corresponding \mathcal{C}^i .

B. Non-Binary EXIT Chart Analysis

We now evaluate the extrinsic information transfer characteristics of the soft detector developed in section V-A, based on the non-binary case. Alexei *et al.* [18] has proved, based on the binary iterative system, that the extrinsic information E_k (the k^{th} time instant) of an *a posteriori* probability (APP) decoder contains the same amount of information as the physical channel outputs \mathbf{Y} and the outputs of the *a priori* channel $\mathbf{Z}_{\setminus k}$. We can prove that when the extrinsic outputs are non-binary-based, this theorem also holds. In this case, E_k becomes the vector-based random variable \mathbf{E}_k , and can be expressed as:

$$I(V_k|\mathbf{E}_k) = I(V_k|\mathbf{Y}, \mathbf{Z}_{\setminus k})$$

The proof [19] is based on the fact that $\Pr(V_k = v|\mathbf{e}_k) = \Pr(V_k = v|\mathbf{y}, \mathbf{z}_{\setminus k})$. The average extrinsic information $I_E = \frac{1}{N} \sum_{k=1}^N I(V_k; \mathbf{E}_k)$ can be obtained by:

Fig. 3(a) illustrates the extrinsic transfer characteristics for a two-level EDC lattice over the TWRC, where $\varpi = 2 + 4\omega = 2(1 + 2\omega)$. Based on the definition of EDC and (64), the linear codes \mathcal{C}^1 and \mathcal{C}^2 are over \mathbb{F}_3 and a binary extension field \mathbb{F}_{2^2} , respectively. The extrinsic information I_e^1 for the linear combinations of the 1st level depends only on the *a priori* information I_a^2 from the 2nd level, and similarly for I_e^2 . It can be observed in Fig. 3(a) that there is an increase of the average extrinsic information I_e^1 around 0.8 at 10dB when the soft detector has the ideal *a priori* information at the 2nd level, compared to the non-iterative case. Hence the iteration-aided multistage detection implies a large potential to improve the reliability of decoding the linear combinations at each level. Due to space limitation for this paper, we

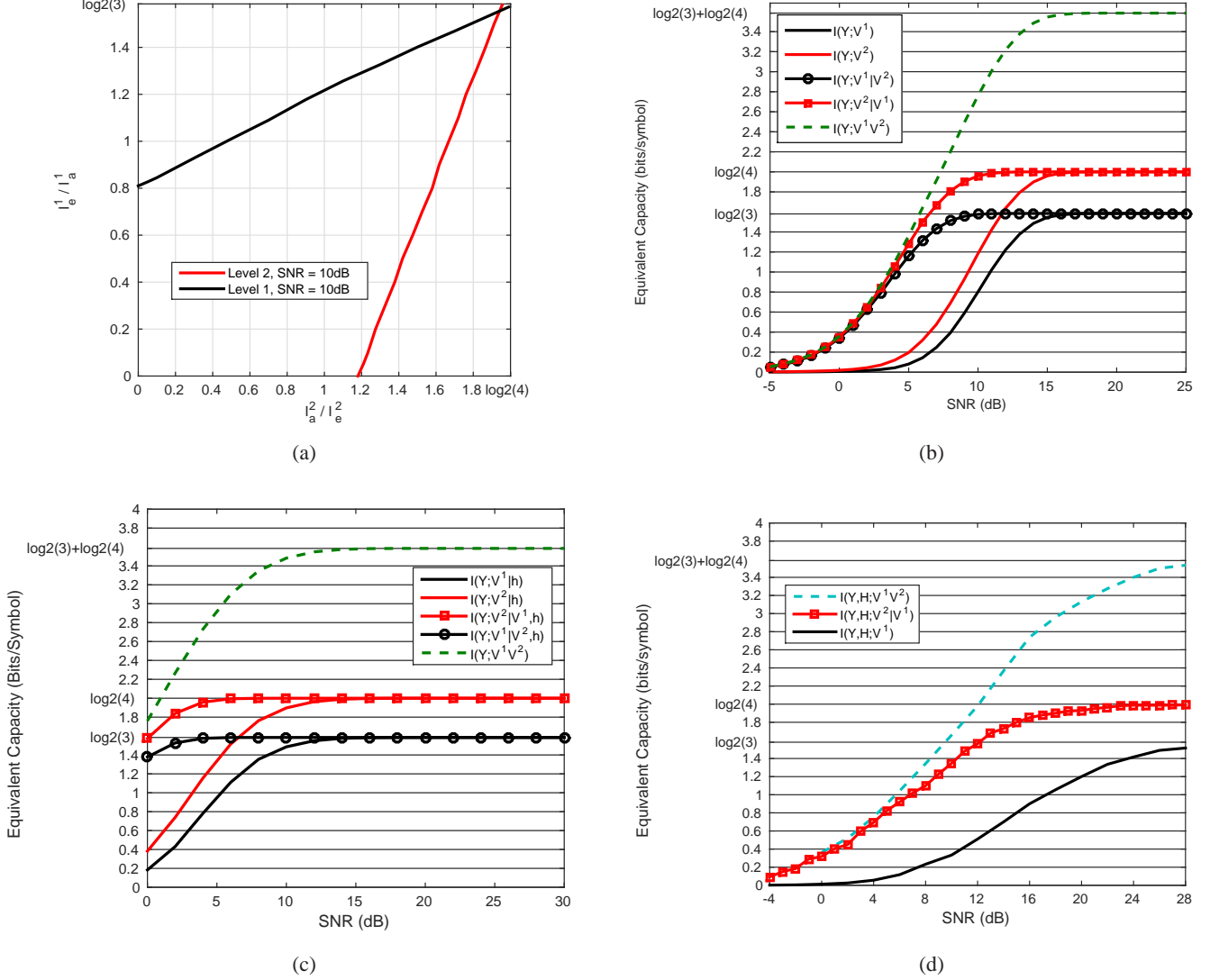


Fig. 3. (a) The EXIT function for each layer. (b) Achievable information rates of the linear combinations at each layer; $h_1 = h_2 = 1$. (c) Achievable rates of the linear combinations at each layer with fixed fading coefficients $h_1 = -1.17 + 2.15 * 1i$ and $h_2 = 1.25 - 1.63 * 1i$. (d) Achievable rates of the linear combinations at each layer with Rayleigh fading.

$$I_E = H(V) + \mathbb{E} \left[\frac{1}{N} \sum_{k=1}^N \sum_{\forall v} \Pr(V_k = v | \mathbf{y}, \mathbf{z}_{\setminus k}) \cdot \log(\Pr(V_k = v | \mathbf{y}, \mathbf{z}_{\setminus k})) \right] \quad (66)$$

show here results only for $h_1 = h_2 = 1$. However the results can be easily extended to the faded MAC. Note that the optimal linear functions f^1, \dots, f^m should be selected in terms of:

$$f^1 \dots f^m = \arg \max_{f^1 \dots f^m} I(Y; V^1 V^2 \dots V^m) \quad (67)$$

which maximizes the achievable rate. Note that V^i is a random variable with its outcomes from the linear function f^i . Hence the conditional probability density $\Pr(Y|V^i)$ is a function of the messages

$w_j^i, j = 1, 2, \dots, L$. Fig. 3(b) gives the numerical integration results for the achievable rates at each level. It can be observed that the mutual information chain rule is satisfied, which gives theoretical support for multistage iterative decoding. Fig. 3(b) also well matches the EXIT chart results in Fig. 3(a), e.g. the extrinsic information of the linear combinations for the first level is around $I(Y; V^1) = 0.8$ and $I(Y; V^1|V^2) = 1$ at 10dB which precisely match the black line in Fig. 3(a). Fig. 3(c) and Fig. 3(d) give the achievable information rates of the linear combinations at each level based on the fixed fading and Rayleigh fading, respectively. The detailed calculation of these are described in Appendix B.

It is seen that the maximum achievable rates for the network coded linear combinations are $\mathcal{R}^{(1)} = \log_2 3$ and $\mathcal{R}^{(2)} = \log_2 4$ for level 1 and 2. The allowable rate at a certain level is higher when the *a priori* information from another layer is available. We assume two memory 3, 1/2-rate convolutional codes are used at both levels (over \mathbb{F}_3 and \mathbb{F}_{2^2} respectively). EDC lattices achieve overall rate $\frac{1}{2} \log_2(12)$, with the number of trellis states 27 and 64 at the corresponding levels. However, a single convolutional code over ring R_{12} needs 1728 trellis states. The complexity reduction is obvious.

VI. SIMULATION RESULTS

In this section, we evaluate the performance of the MLNC scheme, based on the detection approaches proposed. These results give strong support for the Theorems and Lemmas developed in previous sections. In this paper, we focus mainly on the applications of EDC lattices in MLNC. However, it is not necessarily limited to EDC lattices since MLNC design applies in principle to the general case. For example, high coding gain lattice codes (e.g. complex low density lattice codes [4][20] and signal codes [21]) which are directly designed in the geometric space can be used in the MLNC framework. This is interesting and will be investigated in our later work.

We are mainly concerned (in this paper) with the performance of the multiple access channel (MAC) of the TWRC, which can be viewed as the building block for more complicated network topologies. All simulations are based on a two-layer EDC lattice which has the same configuration. Thus, the two layers are constructed via linear codes $\mathcal{C}^1 \in \mathbb{F}_3$ and $\mathcal{C}^2 \in \mathbb{F}_{2^2}$. The linear codes at both layers are non-binary convolutional codes, with their generator polynomials defined in Table I. Note that the decoder of the non-binary convolutional codes is based on the maximum a posteriori (MAP) probability criteria and modified BCJR algorithm, where the soft output of the component symbols is produced. We do not give detailed explanation of the decoding in this paper since it is not our main concern, but we will provide the algorithm when requested. Unless otherwise stated, the convolutional decoder employs the same algorithm in the sequel.

TABLE I
CODE TYPE AND CODE RATE ASSIGNED FOR EACH LEVEL.

i	$g(D)$
1	$[-2\omega^2 + 2\omega^2 D^3, 2\omega^2 + (-2\omega^2)D + 2\omega^2 D^3]$
2	$\begin{bmatrix} -2 + (1 - \omega)D^2 + (-2)D^3 \\ -2 + (-2)D + (-2)D^2 + (1 - \omega^2)D^3 \end{bmatrix}$

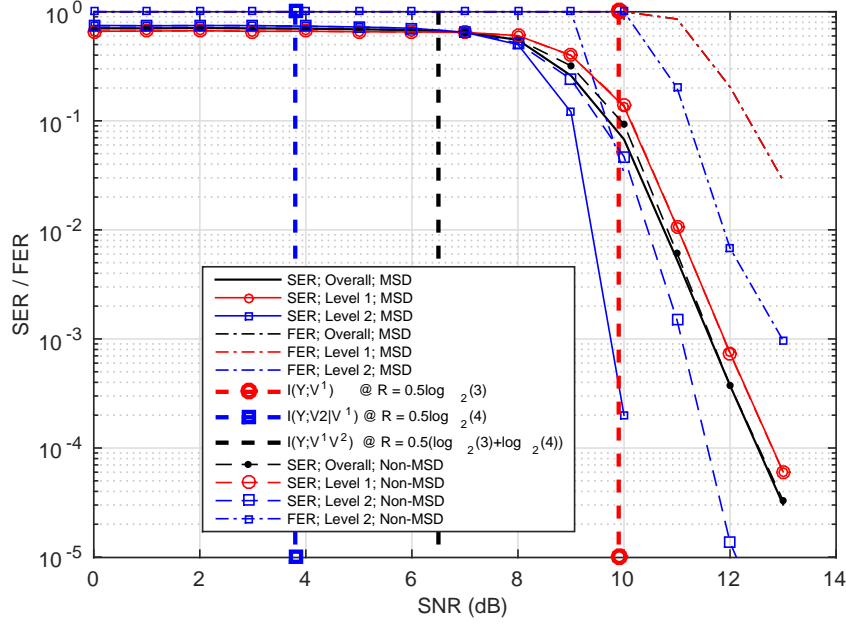


Fig. 4. SER and FER performance for an MLNC constructed from a two layer EDC Lattices; Soft detection; Multistage decoding/Non-Multistage decoding; $\mathcal{R}_{\text{mes}}^{(1)} = \frac{1}{2} \log_2(3)$; $\mathcal{R}_{\text{mes}}^{(2)} = \frac{1}{2} \log_2(4)$; $h_1 = h_2 = 1$.

Fig. 4 depicts the symbol-error rates and frame-error rates for EDC-based MLNC as a function of SNR, where the soft detection approach is used. We examine the performance with and without multistage decoding when iterations and fading are not considered. The convolutional code at the i^{th} level is defined as a $[2(\iota^i + \nu^i), \iota^i]$ linear block code, where ι^i and ν^i denote the data and memory length, respectively. Therefore the overall message rate is given by:

$$\mathcal{R}_{\text{mes}} \approx \frac{1}{2}(\log_2 3 + \log_2 4) \text{ bits/symbol}$$

Note that we use the approximation sign here since the actual coding rate is smaller than $\frac{1}{2}$ due to the tail effect of memory. When the block length is sufficient large, this effect can be ignored. Without multistage decoding, it is observed from Fig. 4 that the SER gap between layer 1 and 2 is around 0.8dB at BER= 10^{-4} , and layer 1 is 8dB from the capacity of layer 1. When multistage decoding is performed

from layer 1 to layer 2, we expect that the SER performance of layer 2 can be improved as a result of the additional *a priori* soft information from layer 1. Note that layer 2 operates over \mathbb{F}_{2^2} whereas its *a priori* soft information is over \mathbb{F}_3 . The simulation results confirm this anticipation in that the SER of layer 2 has 2dB gain over non-MSD at 10^{-5} . However this leads to only slightly better overall performance. When multistage processing starts from layer 1, it is obvious that MSD and non-MSD should give approximately the same performance at layer 1. The overall performance is dominated by the layer which has the worst SER performance over all layers, and in this case, it is layer 1. This explains the reason why the performance improvement of layer 2 gives small contribution in the overall SER.

To further increase network throughputs, and examine the performance of MSD based on the asymmetric coding rates over each level, the rate of layer 2 is set to $\mathcal{R}^{(2)} = \frac{3}{4}$. Thus, the sublattice Λ_{p_2} is constructed via a higher rate linear code. The overall message rate is given by

$$\mathcal{R}_{\text{mes}} \approx \frac{1}{2} \log_2 3 + \frac{3}{4} \log_2 4 \text{ bits/symbol}$$

Note that the SER curve of level 1 (red dashed circle) without MSD should closely match that with MSD (red solid circle) when multistage decoding is used in layer 1. Simulations in Fig. 5 confirm this. Based on the increased coding rate, we are more concerned with the SER performance of layer 2. It is observed from Fig. 5 that the SER performance of layer 2 is greatly degraded if MSD is not employed, with approximately 3dB loss at 10^{-5} compared to the half-rate code used at this level. However, when MSD is used, the SER (blue solid square) of layer 2 has more than 3dB gain over the non-MSD case (blue dashed square) as a result of the reliable *a priori* feedback from layer 1. The overall performance of MSD-based detection is determined mainly by layer 1, whereas for non-MSD-based detection, the overall performance is dominated by layer 2. That is the reason why the overall SER of the MSD-based scheme performs better than the non-MSD scenario, with 2dB gain obtained at 10^{-5} . It is interesting to note that when the decoding of the Λ_{p_i}/Λ' which is constructed from a higher rate linear code occurs at a later stage of MSD, the overall SER performance of MSD over non-MSD performs better. Hence, MSD is particularly suitable for the detection of EDC lattices in terms of MLNC design, since each layer of EDC operates over an asymmetric finite field or finite chain ring. Now the overall SER is 4.5dB from the capacity. Note that the measure of SER is based on the correct recovery of the linear combinations of original messages at each source over the respective algebraic field.

Iterative Multistage Decoding: we believe that there is room to improve SER and FER performance further. Based on the soft detector developed in section V, and also the soft decoder developed for the

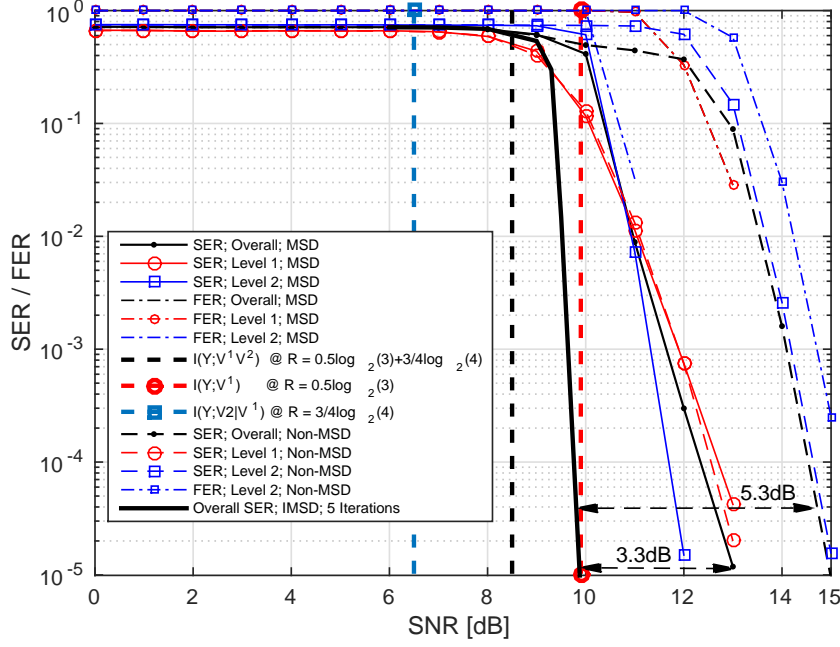


Fig. 5. SER and FER performance for an MLNC constructed from a two layer EDC Lattices; Soft detection; Multistage decoding / Non-Multistage decoding / IMSD; Asymmetric coding rate; $\mathcal{R}_{\text{mes}}^{(1)} = \frac{1}{2} \log_2(3)$; $\mathcal{R}_{\text{mes}}^{(2)} = \frac{3}{4} \log_2(4)$; $h_1 = h_2 = 1$.

non-binary convolutional codes, we propose to apply the iterative technique to EDC-lattice-based MLNC.

Fig. 5 depicts the result when IMSD is used. It is observed that with 5 iterations, the SER curve (black solid thick line) has a sharp turbo cliff reaching $\text{SER} = 10^{-5}$ at 10dB, which is only 1.4dB from the capacity. Thus, iterative decoding gives 3.3dB gain over the traditional MSD decoding, and 5.3dB gain over non-MSD decoding, as shown in the figure. Note that the simulation result is well consistent with the EXIT functions in Fig. 3(a). When sufficient iterations are given, the L-value outputs from the soft detector at both layers are sufficiently reliable that the decoder can make the estimation with small probability of error. The simulation result also validates the soft detector algorithm specifically developed for EDC-based MLNC, and implies that there is large potential in employing iterative decoding in the multilevel lattice network coding.

Layered Integer Forcing: we have presented a general framework for the multilevel lattice network coding in section III. The work implies that any lattices with multilevel structure can be used in MLNC, and the essence of MLNC is to decode each layer separately such that the lattice decoder at each layer operates over smaller finite field or chain ring. The layered integer forcing is a network decoding technique developed in terms of the algebraic structure of MLNC and hence, is generally applicable to any MLNC design. Thus, LIF is in principle capable of decoding EDC-lattice-based MLNC. According to Theorem 3, each layer forms a new quotient S -lattice Λ/Λ'_i , and there exists a surjective S -module homomorphism

φ_i for the i^{th} layer such that $\mathcal{K}(\varphi_i) = \Lambda'_i$. The general form of the generator matrix for Λ'_i based on the EDC lattice is given in (42). Note that Λ'_i is the coarse lattice for the new coset system Λ/Λ'_i .

In order to implement the LIF decoding for EDC lattices, we develop a modified Viterbi detector (see Appendix C) which can be viewed as a lattice quantizer based on the quotient S -lattice Λ/Λ'_i for the i^{th} layer, $i = 1, 2, \dots, m$.

Fig. 6 illustrates the SER and FER performance based on LIF. It is observed (black solid line) that the overall SER has a good slope which validates the correctness of LIF and the modified Viterbi quantizer designed for the EDC lattice. The SER performance of LIF has approximately 0.8dB loss at 10^{-5} in comparison to the soft detection approach. This is what we anticipate. First, the soft detection approach employs the BCJR algorithm for the convolutional decoding, which typically slightly outperforms Viterbi detection. Then, the soft detector developed in section V-A and (68) - (74) outputs the soft information that the BCJR decoder uses to produce more reliable estimation than that for the Viterbi decoder.

The soft detection approach is designed specifically for EDC lattices, and it is not strange to see that it gives better performance than LIF. Despite of this, we emphasise that LIF is universally applicable to any lattices having multilevel structure as detailed in section III, rather than just EDC lattices. For example, LIF is capable of solving MLNC problem when the lattices are directly designed in the Euclidean space (e.g. LDLC and signal codes). In summary, the application of the soft detection approach is more restrictive (which applies only to EDC lattices) and has relatively large complexity, but gives the best performance compared to LIF with Viterbi detection. However, LIF provides a solution for any kind of MLNC problem. Which method is preferable depends on the trade-off of factors relevant to a particular scenario.

In Fig. 7, we also show the performance of the LSD when the fixed fading is considered. The channel fading vector is set to $\mathbf{h} = [-1.17 + 2.15i, 1.25 - 1.63i]$, which is the same as the fading vector used in scenario 1 of [21]. We employ a half-rate code for layer 1, and $\frac{3}{4}$ -rate code for layer 2. The optimal S -integer vector for the two layers are selected in terms of (67). We employ multistage decoding with 5 iterations between the two layers. A sharp turbo cliff occurs, which reaches $\text{SER} = 10^{-5}$ at 3.9dB, approximately 1.7dB from the capacity. When no iteration is employed, there is more than 5dB loss. This implies that small number of additional iterations to generate more reliable values is worthwhile in improving the overall SER performance. The iterative multistage soft detection for EDC lattices achieves the overall rate of $\mathcal{R}_{\text{mes}} \approx 2.29$ bits/symbol at 3.9dB. This demonstrates the potential of iterative decoding in improving the performance of physical layer network coding.

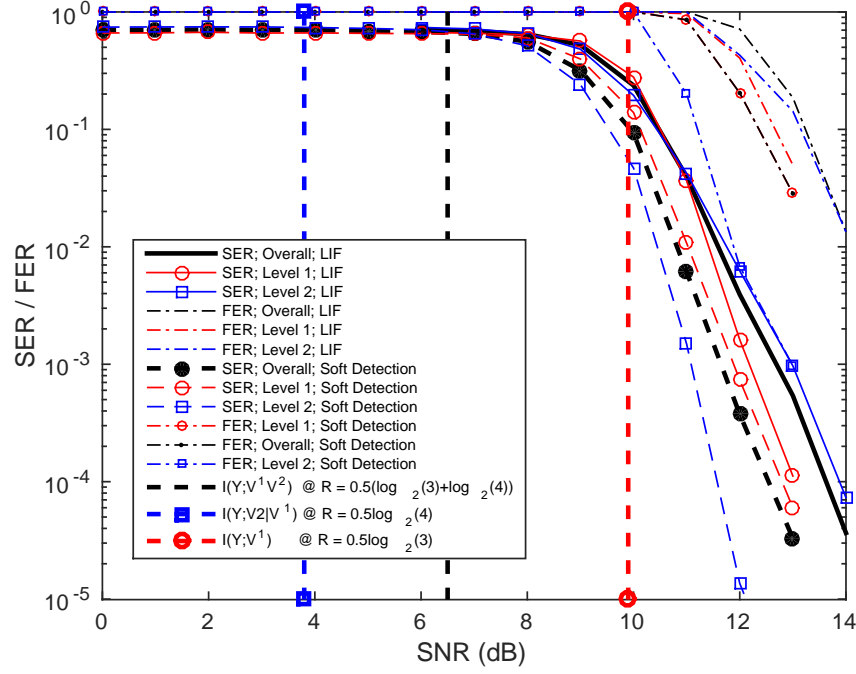


Fig. 6. SER and FER performance for an MLNC constructed from a two layer EDC Lattices; Soft detection; LIF; $\mathcal{R}_{\text{mes}}^{(1)} = \frac{1}{2} \log_2(3)$; $\mathcal{R}_{\text{mes}}^{(2)} = \frac{1}{2} \log_2(4)$; $h_1 = h_2 = 1$.

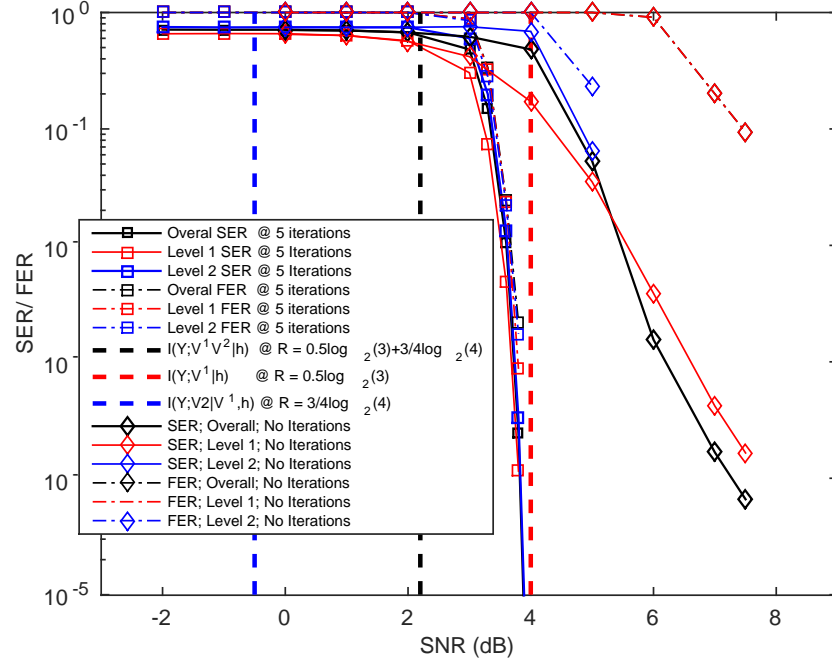


Fig. 7. SER and FER performance for an MLNC constructed from a two layer EDC Lattices; Soft detection; LIF; $\mathcal{R}_{\text{mes}}^{(1)} = \frac{1}{2} \log_2(3)$; $\mathcal{R}_{\text{mes}}^{(2)} = \frac{1}{2} \log_2(4)$; $\mathbf{h} = [-1.17 + 2.15i, 1.25 - 1.63i]$.

VII. CONCLUSIONS

The paper has laid the foundations for a new research area in multilevel lattices for LNC, and built on the theoretic work for MLNC which inherently allows practically feasible decoding design for network coding, and correspondingly we have developed a layered integer forcing approach which plays such a role. We have proposed a general lattice construction, i.e. EDC, based on MLNC theorems, given the generator matrix forms and shown its merits, especially for complexity reduction and code design flexibility. We have considered three possible EDC lattice structures, and mathematically proved that EDC subsumes the most important previous complex constructions, e.g. A and D. We have laid the foundations for another new research area in iteration-aided multistage decoding for EDC-based MLNC, which is based on the layered soft detector developed in section V, and have explored its extrinsic information transfer characteristics. The results well support our viewpoint that LSD works well with multistage iterative decoding in MLNC, and provides better performance than the traditional non-iterative system. We have developed a modified Viterbi decoder based on LIF for EDC-based MLNC, and made performance comparison between iterative decoding, multistage decoding and LIF.

We expect that all of these will provide the basis for extensive further work, both to explore the rich algebraic features of the new construction and the homomorphism design, and to exploit it in practical implementations of LNC in 5G wireless systems.

VIII. ACKNOWLEDGEMENTS

The authors would like to thank Chen Feng from University of Toronto for useful discussions on lattice network coding.

REFERENCES

- [1] U. Erez and R. Zamir, "Achieving $1/2 \log(1+\text{snr})$ on the awgn channel with lattice encoding and decoding," *IEEE Trans. on Inf. Theory*, vol. 50, no. 10, pp. 2293–2314, Oct 2004.
- [2] G. Forney, M. Trott, and S.-Y. Chung, "Sphere-bound-achieving coset codes and multilevel coset codes," *IEEE Trans. on Inf. Theory*, vol. 46, no. 3, pp. 820–850, May 2000.
- [3] S. Zhang, "Hot topic: physical-layer network coding," in *in Proc. of ACM Mobicom*, 2006, pp. 358–365.
- [4] Y. Wang and A. Burr, "Complex low density lattice codes to lattice network coding," in *IEEE International Communications Conference (ICC)*, June 2015.

- [5] B. Nazer and M. Gastpar, "Compute-and-forward: Harnessing interference through structured codes," *IEEE Trans. Inf. Theory*, vol. 57, no. 10, pp. 6463–6486, Oct 2011.
- [6] C. Feng, D. Silva, and F. Kschischang, "An algebraic approach to physical-layer network coding," *IEEE Trans. Inf. Theory*, vol. 59, no. 11, pp. 7576–7596, Nov 2013.
- [7] Q. Sun, J. Yuan, T. Huang, and K. Shum, "Lattice network codes based on eisenstein integers," *IEEE Trans. Commun.*, vol. 61, no. 7, pp. 2713–2725, July 2013.
- [8] N. Tunali, K. Narayanan, J. Boutros, and Y.-C. Huang, "Lattices over eisenstein integers for compute-and-forward," in *Communication, Control, and Computing (Allerton), 2012 50th Annual Allerton Conference on*, Oct 2012, pp. 33–40.
- [9] Y.-C. Huang and K. Narayanan, "Multistage compute-and-forward with multilevel lattice codes based on product constructions," in *Information Theory (ISIT), 2014 IEEE International Symposium on*, June 2014, pp. 2112–2116.
- [10] D. G. Northcott, *Lessons on Rings, Modules and Multiplicities*, 1968.
- [11] C. Feng, R. Nobrega, F. Kschischang, and D. Silva, "Communication over finite-chain-ring matrix channels," *IEEE Trans. Inf. Theory*, vol. 60, no. 10, pp. 5899–5917, Oct 2014.
- [12] B. R. McDonald, *Finite Rings with Identity*, 1974.
- [13] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, 1998.
- [14] U. Wachsmann, R. Fischer, and J. Huber, "Multilevel codes: theoretical concepts and practical design rules," *IEEE Trans. Inf. Theory*, vol. 45, no. 5, pp. 1361–1391, Jul 1999.
- [15] A. Burr and T. Lunn, "Block-coded modulation optimized for finite error rate on the white Gaussian noise channel," *IEEE Trans. Inf. Theory*, vol. 43, no. 1, pp. 373–385, Jan. 1997.
- [16] Y. H. Gan, C. Ling, and W. H. Mow, "Complex lattice reduction algorithm for low-complexity full-diversity mimo detection," *IEEE Trans. Sig. Processing*, vol. 57, no. 7, pp. 2701–2710, July 2009.
- [17] Y. Wang and A. Burr, "Code design for iterative decoding of multilevel codes," *IEEE Trans. Commun.*, vol. 63, no. 7, pp. 2404–2419, July 2015.
- [18] A. Ashikhmin, G. Kramer, and S. ten Brink, "Extrinsic information transfer functions: model and erasure channel properties," *IEEE Trans. Inf. Theory*, vol. 50, pp. 2657–2673, Nov 2004.
- [19] J. Klierer, S. X. Ng, and L. Hanzo, "Efficient computation of exit functions for nonbinary iterative decoding," *IEEE Trans. Inf. Commun.*, vol. 54, no. 12, pp. 2133–2136, Dec 2006.
- [20] Y. Yona and M. Feder, "Complex low density lattice codes," in *Information Theory Proceedings*

(ISIT), 2010 IEEE International Symposium on, Jun. 2010, pp. 1027–1031.

- [21] O. Shalvi, N. Sommer, and M. Feder, “Signal codes: Convolutional lattice codes,” *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 5203–5226, Aug 2011.

APPENDIX A

LAYERED SOFT DETECTOR FOR EDC-BASED MLNC

We show here the calculation of mutual information/ conditional mutual information between the received superimposed signals (faded and noisy) and the network coded symbols at the j^{th} level. We denote by $\mathbf{w}_j = [w_j^1, \dots, w_j^m]$, $j = 1, 2, \dots, L$ the realizations of a vector-based random variable \mathbf{W}_j representing the messages of all m levels at the j^{th} source, and $\mathbf{w}^i = [w_1^i, \dots, w_L^i]$, $j = 1, 2, \dots, m$ the realizations of a vector-based random variable W^i representing the messages of all L sources for the i^{th} level. We refer to $\mathbf{w} = [\mathbf{w}_1, \dots, \mathbf{w}_L]$ as the realizations of another vector-based random variable \mathbf{W} . Note that $w_j^i \in \mathbb{F}_{\tilde{p}_i}$ is the message of the i^{th} level and the j^{th} source, which is uniformly distributed over $\mathbb{F}_{\tilde{p}_i}$. V^i is a random variable which takes on a set of possible values of $f^i(w_1^i, \dots, w_L^i) \in \mathbb{F}_{\tilde{p}_i}$, and v^i is the corresponding realization of V^i for the i^{th} layer.

The *a posteriori* probability of the event $V^i = v^i$ at the i^{th} level conditioned on the MAC outputs $Y = y$ and the *a priori* channel outputs $\Xi = \xi = [\xi^1, \dots, \xi^m]$, is given by

$$\Pr(V^i = v^i | y, \xi) \tag{68}$$

$$= \sum_{V^i = v^i} \sum_{\mathbf{V}^{\setminus i} \in \mathbb{F}_{\mathbf{q}^{\setminus i}}^{m-1}} \frac{\Pr(Y | V^1 \dots V^m, \xi) \Pr(\xi | V^1 \dots V^m) \Pr(V^1 \dots V^m)}{\Pr(Y, \xi)} \tag{69}$$

$$= \Pr(\xi^i | V^i = v) \sum_{V^i = v} \cdot \sum_{\mathbf{V}^{\setminus i} \in \mathbb{F}_{\mathbf{q}^{\setminus i}}^{m-1}} \frac{\Pr(Y | V^1 \dots V^m) \Pr(\xi^{\setminus i} | \mathbf{V}^{\setminus i}) \Pr(V^1 \dots V^m)}{\Pr(Y, \xi)} \tag{70}$$

$$= \frac{\Pr(\xi^i | V^i = v)}{\Pr(Y, \xi)} \sum_{\substack{\forall (w_1^i, \dots, w_L^i): \\ f^i(w_1^i, \dots, w_L^i) = v}} \cdot \sum_{\mathbf{V}^{\setminus i} \in \mathbb{F}_{\mathbf{q}^{\setminus i}}^{m-1}} \cdot \sum_{\substack{\forall (\mathbf{w}_1^{\setminus i}, \dots, \mathbf{w}_L^{\setminus i}): \\ f^1(\mathbf{w}_1^{\setminus i}) = v^1, \dots, f^m(\mathbf{w}_m^{\setminus i}) = v^m}} \Pr(Y | \mathbf{W} = \mathbf{w}) \Pr(\xi^{\setminus i} | \mathbf{V}^{\setminus i}) \Pr(\mathbf{W} = \mathbf{w}) \tag{71}$$

where $\mathbb{F}_{\mathbf{p}^{\setminus i}}^{m-1} \triangleq [\mathbb{F}_{\tilde{p}_1} \dots \mathbb{F}_{\tilde{p}_{i-1}}, \mathbb{F}_{\tilde{p}_{i+1}} \dots \mathbb{F}_{\tilde{p}_m}]$ consists of a set of finite field and finite chain ring. $\mathbb{F}_{\tilde{p}_i}$ is defined in section IV-A. Note that if \tilde{p}_i is not a prime number, $\mathbb{F}_{\tilde{p}_i}$ can be decomposed furthermore in terms of the p -adic decomposition theorem [11], and small modifications of (71) are required accordingly.

The conditional probability density function is given by,

$$\begin{aligned}
& \Pr(Y|\mathbf{W} = \mathbf{w}) \\
&= \Pr(Y|\mathbf{w}_1, \dots, \mathbf{w}_L) \\
&= \frac{1}{\sqrt{\pi N_0}} e^{-\frac{|h_1 \sigma^{-1}(\mathbf{w}_1^1 \times \dots \times \mathbf{w}_1^m) + \dots + h_L \sigma^{-1}(\mathbf{w}_L^1 \times \dots \times \mathbf{w}_L^m) - y|^2}{N_0}}
\end{aligned} \tag{72}$$

The *a posteriori* L-value d_k^i for the event $V^i = v_k^i$ is defined in (73) which can be further separated into two terms in (74), where a_k^i is an element in (65) which serves as the *a priori* L-value. Note that v_k^i is the k^{th} realization of the random variable V^i . Following (65), we have

$$\Pr(\xi|V = v_k^i) = \frac{e^{a_k^i}}{1 + \sum_{k: \forall v_k^i \in \mathbb{F}_{\bar{p}_i}, v_k^i \neq 0} e^{a_k^i}}$$

The second term of (74) serves as the extrinsic L-value e_k^i for the i^{th} level and the k^{th} realization of the vector-based random variable \mathbf{E}^i which is the extrinsic information of the i^{th} level.

$$d_k^i = \log \left(\frac{\Pr(V^i = v_k^i | y, \boldsymbol{\xi})}{\Pr(V^i = 0 | y, \boldsymbol{\xi})} \right) \tag{73}$$

$$\begin{aligned}
&= a_k^i + \log \left(\frac{\sum_{f^i(w_1^i, \dots, w_L^i): f^i(w_1^i, \dots, w_L^i) = v_k^i} \cdot \sum_{\forall \mathbf{V}^i \in \mathbb{F}_{\mathbf{q}^i}} \cdot \sum_{f^1(\mathbf{w}^1) = v^1, \dots, f^m(\mathbf{w}^m) = v^m} \Pr(Y|\mathbf{W} = \mathbf{w}) \Pr(\boldsymbol{\xi}^i | \mathbf{V}^i)}{\sum_{f^i(w_1^i, \dots, w_L^i) = 0} \cdot \sum_{\forall \mathbf{V}^i \in \mathbb{F}_{\mathbf{q}^i}} \cdot \sum_{f^1(\mathbf{w}^1) = v^1, \dots, f^m(\mathbf{w}^m) = v^m} \Pr(Y|\mathbf{W} = \mathbf{w}) \Pr(\boldsymbol{\xi}^i | \mathbf{V}^i)} \right)
\end{aligned} \tag{74}$$

$$= a_k^i + e_k^i$$

APPENDIX B

MUTUAL INFORMATION FOR LINEAR COMBINATIONS

The mutual information between the received signal and the decoded linear combination at the i^{th} layer is:

$$\begin{aligned}
I(Y, H; V^i) &= \mathbf{E}_{(Y, V^i, H)} \left[\log_2 \frac{P(Y|V^i, H)}{P(Y)} \right] \\
&= \sum_{v^i} \Pr(V^i = v_i) \int_{\mathbb{C}} P(H) \int_{\mathbb{C}} P(Y|V^i, H) \log_2 \frac{P(Y|V^i, H)}{P(Y)} dY dH
\end{aligned} \tag{75}$$

The probability density function $P(Y|V^i, H)$ conditioned on $V^i = v^i$ should be calculated by:

$$P(Y|V^i = v^i, H) = \frac{1}{\Pr(V^i = v^i)} \sum_{\forall \mathbf{v} \setminus i} \sum_{\substack{\forall (\mathbf{w}_1, \dots, \mathbf{w}_L): \\ f^1(\mathbf{w}^1) = v^1, \dots, f^m(\mathbf{w}^m) = v^m}} P(Y|\mathbf{W} = \mathbf{w}, h) P(\mathbf{W} = \mathbf{w}) \quad (76)$$

The conditional mutual information $I(Y; V^i | V^1 \dots V^{i-1})$ gives the maximum achievable rate at the i^{th} layer when the linear combinations of the preceding stages are perfectly known, which can be calculated by:

$$\begin{aligned} & I(Y; V^i | V^1 \dots V^{i-1}) \\ &= \mathbf{E}_{(Y, V^1, \dots, V^i, H)} \left[\log_2 \frac{P(Y|V^1 \dots V^i, H)}{P(Y|V^1 \dots V^{i-1}, H)} \right] \\ &= \sum_{v^1 \dots v^{i-1}} \Pr(V^1 = v^1, \dots, V^{i-1} = v^{i-1}) \sum_{v^i} \int_{\mathbb{C}} P(H) \int_{\mathbb{C}} P(Y, V^i | V^1 \dots V^{i-1}, H) \log_2 \frac{P(Y|V^1 \dots V^i, H)}{P(Y|V^1 \dots V^{i-1}, H)} dY dH \end{aligned} \quad (77)$$

where the conditional probability density function $P(Y, V^i | V^1 \dots V^{i-1}, H)$ should be calculated in terms of the random variables of the messages, which is given by:

$$\begin{aligned} & P(Y, V^i | V^1 = v^1, \dots, V^{i-1} = v^{i-1}, H) \\ &= \frac{1}{\Pr(v^1, \dots, v^{i-1})} \sum_{\forall \mathbf{v} \notin (v^1 \dots v^i)} \sum_{\substack{\forall (\mathbf{w}_1, \dots, \mathbf{w}_L): \\ f^1(\mathbf{w}^1) = v^1, \dots, f^m(\mathbf{w}^m) = v^m}} P(Y|\mathbf{W} = \mathbf{w}, h) \Pr(\mathbf{W} = \mathbf{w}) \end{aligned} \quad (78)$$

where $P(Y|\mathbf{W} = \mathbf{w}, h)$ is given in (72). Note that V^i , $i = 1, 2, \dots, m$ is a random variable defined by the linear function of the i^{th} layer over $\mathbb{F}_{\tilde{p}_i}$. Every V^i operates over different finite field or chain ring.

APPENDIX C

LIF QUANTIZER

We show here a LIF quantizer $\mathcal{Q}_{\text{LIF}}^{(i)}$ implemented via a modified Viterbi decoder. The quantization problem for the i^{th} layer can be mathematically expressed as:

$$\arg \min_{\mathbf{c}_i} \|\alpha^i \mathbf{y} - (\tilde{\sigma}^{-1}(\mathbf{c}^i) + \lambda'_i)\|^2 \quad (79)$$

$$= \arg \min_{\mathbf{c}_i} \|(\alpha^i \mathbf{y} - \tilde{\sigma}^{-1}(\mathbf{c}^i)) - \mathcal{Q}_{\Lambda'_i}((\alpha^i \mathbf{y} - \tilde{\sigma}^{-1}(\mathbf{c}^i)))\|^2 \quad (80)$$

$$\text{subject to :} \quad \mathbf{c}^i \in \mathcal{C}^i, \quad \lambda'_i \in \Lambda'_i, \quad (81)$$

$$\tilde{\sigma}(\lambda) \in \mathcal{C}^1 \oplus \dots \oplus (\mathcal{C}^i = \mathcal{C}^i) \oplus \dots \mathcal{C}^m \quad (82)$$

where $\mathcal{Q}_{\Lambda'_i}(\mathbf{x})$ is the coarse lattice quantizer for the i^{th} layer and can be expressed as a modulo operation $\mathbf{x} \bmod \Lambda'_i$ (as defined in Theorem 3). $\tilde{\sigma}^{-1}(\cdot)$ is the inverse operation of $\tilde{\sigma}$ which produces a set of lattice points λ .

We can construct trellis for the non-binary convolutional code \mathcal{C}^i . Assume that the states of the k^{th} and $(k+1)^{\text{th}}$ time slots are s_k and s_{k+1} , respectively. The codeword of the branch that exists from s_k and arrives at s_{k+1} is denoted as $c_{s_k \rightarrow s_{k+1}}^i$. The metric for each branch is given by

$$\|(\alpha^i \mathbf{y} - \sigma^{-1}(c_{s_k \rightarrow s_{k+1}}^i)) - \mathcal{Q}_{\Lambda'_i}(\alpha^i \mathbf{y} - \sigma^{-1}(c_{s_k \rightarrow s_{k+1}}^i))\|^2 \quad (83)$$

where $\sigma^{-1}(\cdot)$ is the inverse operation of $\sigma(\cdot)$ defined in section IV-A. We employ Viterbi algorithm to estimate the best possible outcome \mathbf{c}^i . This implements the LIF quantizer $\mathcal{Q}_{\text{LIF}}^{(i)}$ for EDC-based MLNC.

APPENDIX D

PROOF OF PROPOSITIONS 1 AND 2

The codeword of the i^{th} layer is $\mathbf{c}^i = (c_1^i + \langle \varpi \rangle, \dots, c_n^i + \langle \varpi \rangle) \in \mathcal{C}^i$. \mathcal{C}^i is a linear code over $\delta_i S / \langle \varpi \rangle$ which is generated by $\tilde{\sigma}_i([\mathbf{I}_{k_i} \quad \mathbf{B}_{k_i \times (n-k_i)}^i])$ where $[\mathbf{I}_{k_i} \quad \mathbf{B}_{k_i \times (n-k_i)}^i]$ is a $k_i \times n$ matrix over $\delta_i S$. These are defined in (36) and (37). The minimum-norm coset leader in the i^{th} layer primary sublattice system is given by:

$$\begin{aligned} \tilde{\sigma}_{i,\Delta}(\mathbf{c}^i) &= (c_1^i - \mathcal{Q}_i(c_1^i/p_i\delta_i)p_i\delta_i, \dots, c_n^i - \mathcal{Q}_i(c_n^i/p_i\delta_i)p_i\delta_i) \\ &= (c_1^i - \varpi \mathcal{Q}_i(c_1^i/\varpi), \dots, c_n^i - \varpi \mathcal{Q}_i(c_n^i/\varpi)) \end{aligned} \quad (84)$$

where $\mathcal{Q}(z)$ is a quantizer which sends $z \in \mathbb{C}$ to the closest point in S . We denote $d^2(\Lambda_{p_i}/\Lambda')$ as the length of the squared shortest vectors in the set $\Lambda_{p_i} \setminus \Lambda'$, then

$$d^2(\Lambda_{p_i}/\Lambda') = \min_{\mathbf{c}^i \neq \mathbf{0}, \mathbf{c}^i \in \mathcal{C}^i} \|\tilde{\sigma}_{i,\Delta}(\mathbf{c}^i)\|^2 = \omega_{\min}^{(i)}(\mathcal{C}^i) \quad (85)$$

The volume of the Voronoi region of Λ' is $V(\mathcal{V}(\Lambda')) = \vartheta^n |\varpi|^{2n}$, where ϑ is a scaling factor depending on which PID is used, e.g., $\vartheta = \sqrt{3}/2$ when S is Eisenstein integer. The nominal coding gain for the i^{th}

layer primary sublattices is:

$$\begin{aligned}
\varrho(\Lambda_{p_i}/\Lambda') &= \frac{\omega_{\min}^{(i)}(\mathcal{C}^i)}{(V(\mathcal{V}(\Lambda_{p_i})))^{\frac{1}{n}}} \\
&= \frac{\omega_{\min}^{(i)}(\mathcal{C}^i)}{(\vartheta^n |p_i|^{2(n-k_i)} |\delta_i|^{2n})^{\frac{1}{n}}} \\
&= \frac{\omega_{\min}^{(i)}(\mathcal{C}^i)}{\vartheta |p_i|^{2(1-\frac{k_i}{n})} |\delta_i|^2}
\end{aligned} \tag{86}$$

We now prove the kissing number for the i^{th} layer primary sublattices. Let $N(\omega_{\min}^{(i)}(\mathcal{C}^i))$ be the number of codewords in \mathcal{C}^i with the minimum Euclidean weight $\omega_{\min}^{(i)}(\mathcal{C}^i)$, and $\mathcal{N}_{\mathcal{U}(S)}$ be the number of units in S , e.g. $\mathcal{N}_{\mathcal{U}(\mathbb{Z}([\omega]))} = 6$. When $|p_i|^2 - 1 \leq \mathcal{N}_{\mathcal{U}(S)}$, recall that \mathcal{C}^i is a linear code over $\delta_i S / \langle \varpi \rangle$. The number of non-zero elements of coset leaders in $\delta_i S / \langle \varpi \rangle$ is $|p_i|^2 - 1$, and these elements must be a subset of $\delta_i \mathcal{U}(S)$. Hence there are $\frac{\mathcal{N}_{\mathcal{U}(S)}}{|p_i|^2 - 1}$ elements in the coset leaders which are formed by the same codeword and give the shortest vector. This means the number of the non-zero elements in a codeword is precisely $\frac{\omega_{\min}^{(i)}(\mathcal{C}^i)}{|\delta_i|^2}$. When $|p_i|^2 - 1 > \mathcal{N}_{\mathcal{U}(S)}$, every neighbour point is represented by different codewords, and hence the kissing number of the i^{th} layer primary sublattices is given by:

$$K(\Lambda_{p_i}/\Lambda') = \begin{cases} N(\omega_{\min}^{(i)}(\mathcal{C}^i)) \left(\frac{\mathcal{N}_{\mathcal{U}(S)}}{|p_i|^2 - 1} \right)^{\frac{\omega_{\min}^{(i)}(\mathcal{C}^i)}{|\delta_i|^2}}, & |p_i|^2 - 1 \leq \mathcal{N}_{\mathcal{U}(S)} \\ N(\omega_{\min}^{(i)}(\mathcal{C}^i)), & \text{Otherwise} \end{cases} \tag{87}$$

and now proposition 1 is proved.

From the proof of Theorem 1, we have $\tilde{\mathbf{c}} = \mathbf{c}^1 + \mathbf{c}^2 + \dots + \mathbf{c}^m$, $\tilde{\mathbf{c}} \in \tilde{\mathcal{C}}$ and $\tilde{\mathcal{C}} \in (S/\langle \varpi \rangle)^n$. The minimum-norm coset leader for Λ/Λ' can be represented by codewords used for all layers, thus:

$$\tilde{\sigma}_{\Delta}(\tilde{\mathbf{c}}) = \left(\tilde{c}_1 - \varpi \mathcal{Q}\left(\frac{\tilde{c}_1}{\varpi}\right), \dots, \tilde{c}_n - \varpi \mathcal{Q}\left(\frac{\tilde{c}_n}{\varpi}\right) \right) \tag{88}$$

where $\tilde{c}_j = c_j^1 + c_j^2 + \dots + c_j^m$ and c_j^i , $j = 1, 2, \dots, n$, $i = 1, 2, \dots, m$, denotes the j^{th} element of the codeword \mathbf{c}^i . Then, the squared shortest vectors in the set $\Lambda \setminus \Lambda'$ can be represented by the m linear codes used at each layer,

$$d^2(\Lambda/\Lambda') = \min_{\tilde{\mathbf{c}} \neq \mathbf{0}, \tilde{\mathbf{c}} \in \tilde{\mathcal{C}}} \|\tilde{\sigma}_{\Delta}(\tilde{\mathbf{c}})\|^2 = \omega_{\min}(\tilde{\mathcal{C}})$$

The nominal coding gain for Λ/Λ' is

$$\begin{aligned}\varrho(\Lambda/\Lambda') &= \frac{\omega_{\min}(\tilde{\mathcal{C}})}{(V(\mathcal{V}(\Lambda)))^{\frac{1}{n}}} \\ &= \frac{\omega_{\min}(\tilde{\mathcal{C}}) \prod_{\ell=2}^m |p_\ell|^{\frac{2(k_\ell - k_1)}{n}}}{\vartheta |p_1|^{2(1 - \frac{k_1}{n})} |\delta_1|^2}\end{aligned}\quad (89)$$

where we assume $k_1 \leq k_2 \leq \dots \leq k_m$ in (89). Let $N(\omega_{\min}(\tilde{\mathcal{C}}))$ be the number of codewords in $\tilde{\mathcal{C}}$ with the minimum Euclidean weight $\omega_{\min}(\tilde{\mathcal{C}})$, the kissing number of this kind of lattices is:

$$K(\Lambda/\Lambda') = N(\omega_{\min}(\tilde{\mathcal{C}})) \quad (90)$$

proposition 2 is thereby proved.

APPENDIX E

PROOF OF PROPOSITIONS 3 AND 4

As explained in section IV-A, the codeword \mathcal{C}^i of the i^{th} layer operates over the finite chain ring $\mathcal{C}^i \in \delta_i S / \langle \varpi \rangle$, where $\delta_i = \varpi / p_i^{\gamma_i}$. Following (43), $\tilde{\sigma}_i(\mathbf{w}^i \mathbf{G}_{\text{FCR}}^i) \mapsto (\delta_i S / \langle \varpi \rangle)^n$, here the message space of the i^{th} layer is defined as:

$$\mathbf{W}^i \cong (\delta_i S / p_i^{\gamma_i} \delta_i S)^{k'_{i,0}} \oplus \dots \oplus (\delta_i S / p_i \delta_i S)^{k'_{i,\gamma_i-1}}$$

Then the minimum-norm coset leader of Λ_{p_i}/Λ' has similar form as (84) with $\mathbf{c}^i \in \mathcal{C}^i$. The nominal coding gain $\varrho(\Lambda_{p_i}/\Lambda')$ can be obtained based on the same derivation in (85) and (86). We are more interested in constructing the primary sublattices with some linear codes over the finite field. This can be implemented via the complex construction D approach, based on a set of nested linear codes, as proved in section IV-A. The residue field is now defined as $Q \triangleq \delta_i S / \langle p_i \delta_i \rangle$. Let $\mathcal{C}^{i,0} \subseteq \dots \subseteq \mathcal{C}^{i,\gamma_i-1}$ be nested linear codes of length n over Q , where $\mathcal{C}^{i,t}$ is an $[n, \sum_{\ell=0}^t k'_{i,\ell}]$ linear code for the t^{th} level of the i^{th} layer, $t = 0, 1, \dots, \gamma_i - 1$. Note that $\mathcal{C}^{i,t}$ is row spanned by the vector space:

$$\mathbf{g}_{\mathcal{C}^{i,t}} = \begin{bmatrix} \mathbf{g}_{k'_{i,0}}^i \\ \mathbf{g}_{k'_{i,1}}^i \\ \vdots \\ \mathbf{g}_{k'_{i,t}}^i \end{bmatrix} \quad (91)$$

where $\mathbf{g}_{k'_{i,t}}^i \in Q_{k'_{i,t} \times n}$. None of the rows of $\mathbf{g}_{\mathcal{C}^i,t}$ are linear combination of the other rows. It is obvious that the primary sublattice point $\lambda_{p_i} \in \Lambda_{p_i} \setminus \Lambda'$ is given by:

$$\lambda_{p_i} = \underbrace{p_i^{\gamma_i} \delta_i \mathbf{s} + p_i^{\gamma_i-1} \mathbf{c}^{i,\gamma_i-1}}_{\Lambda_{p_i}^{\gamma_i-1}} + \dots + p_i \mathbf{c}^{i,1} + \mathbf{c}^{i,0} \quad (92)$$

$$\underbrace{\hspace{10em}}_{\Lambda_{p_i}^0}$$

where $\mathbf{c}^{i,t}$ must not be zero for all possible t values. The outer lattice $\Lambda_{p_i}^{\gamma_i-1} = \{p_i^{\gamma_i-1}(p_i \delta_i \mathbf{s} + \mathbf{c}^{i,\gamma_i-1}) = p_i^{\gamma_i-1} \Lambda_{i,\gamma_i-1}^\perp : \mathbf{s} \in S^n, \mathbf{c}^{i,\gamma_i-1} \in Q^n \setminus \mathbf{0}\}$. Here $\Lambda_{i,\gamma_i-1}^\perp$ forms a lattice which has the same structure as the one in scenario 1, with $\Lambda_{i,\gamma_i-1}^{\perp'} = \{p_i \delta_i \mathbf{s} : \mathbf{s} \in S^n\}$. Thus, $\mathbf{c}^{i,t} = (c_1^{i,t} + \langle p_i \delta_i \rangle, \dots, c_n^{i,t} + \langle p_i \delta_i \rangle) \in \mathcal{C}^{i,t}$. The minimum-norm coset leader for $\Lambda_{i,\gamma_i-1}^\perp / \Lambda_{i,\gamma_i-1}^{\perp'}$ and the minimum Euclidean weight $\omega_{\min}^{(i,\gamma_i-1)}(\mathcal{C}^{i,\gamma_i-1})$ can be readily obtained in the same way as (84) and (85). It is obvious that $\lambda_{p_i}^{\gamma_i-1} \in p_i^{\gamma_i-1} \Lambda_{i,\gamma_i-1}^\perp \setminus p_i^{\gamma_i-1} \Lambda_{i,\gamma_i-1}^{\perp'}$ and we have $\|\lambda_{p_i}^{\gamma_i-1}\|^2 \geq |p_i^{\gamma_i-1}|^2 \omega_{\min}^{(i,\gamma_i-1)}(\mathcal{C}^{i,\gamma_i-1})$. The squared shortest vectors of the inner lattice, e.g. $\|\lambda_{p_i}^0\|^2$ must be at least larger than $\|\lambda_{i,0}^\perp\|^2$ where $\Lambda_{i,0}^\perp \triangleq \{\lambda_{i,0}^\perp = p_i \delta_i \mathbf{s} + \mathbf{c}^{i,0} : \mathbf{s} \in S^n, \mathbf{c}^{i,0} \in Q^n \setminus \mathbf{0}\}$, and we have $\|\lambda_{p_i}^0\|^2 \geq \omega_{\min}^{(i,0)}(\mathcal{C}^{i,0})$. The squared shortest vectors in the set $\Lambda_{p_i} \setminus \Lambda'$ is therefore lower bounded by

$$d^2(\Lambda_{p_i} / \Lambda') \geq \min_{0 \leq t \leq \gamma_i-1} \{|p_i|^{2t} \omega_{\min}^{(i,t)}(\mathcal{C}^{i,t})\}$$

where $\omega_{\min}^{(i,t)}(\mathcal{C}^{i,t})$ is referred to as the minimum Euclidean weight of non-zero codewords in $\mathcal{C}^{i,t} \in Q^n$ (an $[n, \sum_{\ell=0}^t k'_{i,\ell}]$ linear code) for the t^{th} level of the i^{th} layer. The nominal coding gain for the i^{th} layer primary sublattices in scenario 2 is lower bounded by:

$$\begin{aligned} \varrho(\Lambda_{p_i} / \Lambda') &\geq \frac{\min_{0 \leq t \leq \gamma_i-1} \{|p_i|^{2t} \omega_{\min}^{(i,t)}(\mathcal{C}^{i,t})\}}{(V(\mathcal{V}(\Lambda_{p_i})))^{\frac{1}{n}}} \\ &= \frac{|p_i|^{2 \sum_{t=0}^{\gamma_i-1} (\gamma_i-t) \frac{k'_{i,t}}{n}} \min_{0 \leq t \leq \gamma_i-1} \{|p_i|^{2t} \omega_{\min}^{(i,t)}(\mathcal{C}^{i,t})\}}{\vartheta |\varpi|^2} \end{aligned} \quad (93)$$

Let $N_t(\omega_{\min}^{(i,t)}(\mathcal{C}^{i,t}))$ be the number of codewords in $\mathcal{C}^{i,t}$ with the minimum Euclidean weight $\omega_{\min}^{(i,t)}(\mathcal{C}^{i,t})$ for the t^{th} level and the i^{th} layer. The kissing number of the i^{th} layer primary sublattice is upper bounded by

$$K(\Lambda_{p_i} / \Lambda') \leq \begin{cases} \sum_{t=0}^{\gamma_i-1} N_t(\omega_{\min}^{(i,t)}(\mathcal{C}^{i,t})) \left(\frac{\mathcal{N}_{\mathcal{U}(S)}}{|p_i|^2-1} \right)^{\frac{\omega_{\min}^{(i,t)}(\mathcal{C}^{i,t})}{|\delta_i|^2}}, & |p_i|^2 - 1 \leq \mathcal{N}_{\mathcal{U}(S)} \\ \sum_{t=0}^{\gamma_i-1} N_t(\omega_{\min}^{(i,t)}(\mathcal{C}^{i,t})), & \text{Otherwise} \end{cases} \quad (94)$$

This completes the proof of Proposition 3.

We now define the code \mathcal{C}^i such that $\mathbf{c}^i = \mathbf{c}^{i,0} + p_i \mathbf{c}^{i,1} + \dots + p_i^{\gamma_i-1} \mathbf{c}^{i,\gamma_i-1}$, and hence $\mathcal{C}^i \in \delta_i S / \langle \varpi \rangle$. From the theorems developed in sections III and IV-A, we are able to generate a new code $\tilde{\mathcal{C}}$ such that $\tilde{\mathbf{c}} = \mathbf{c}^1 + \dots + \mathbf{c}^m$ which makes $\tilde{\mathcal{C}} \in S / \langle \varpi \rangle$. Thus, the codeword of $\tilde{\mathcal{C}}$ is generated by the nested linear codes $\mathcal{C}^{i,t}$ of all layers. The minimum-norm coset leader for Λ / Λ' can be represented by:

$$\tilde{\sigma}_\Delta(\tilde{\mathbf{c}}) = \left(\tilde{c}_1 - \varpi \mathcal{Q}\left(\frac{\tilde{c}_1}{\varpi}\right), \dots, \tilde{c}_n - \varpi \mathcal{Q}\left(\frac{\tilde{c}_n}{\varpi}\right) \right) \quad (95)$$

where $\tilde{c}_j = c_j^1 + c_j^2 + \dots + c_j^m$ and c_j^i , $j = 1, 2, \dots, n$, $i = 1, 2, \dots, m$, denotes the j^{th} element of the codeword \mathbf{c}^i . Then, the squared shortest vectors in the set $\Lambda \setminus \Lambda'$ can be represented by the m linear codes used at each layer,

$$d^2(\Lambda / \Lambda') = \min_{\tilde{\mathbf{c}} \neq \mathbf{0}, \tilde{\mathbf{c}} \in \tilde{\mathcal{C}}} \|\tilde{\sigma}_\Delta(\tilde{\mathbf{c}})\|^2 = \omega_{\min}(\tilde{\mathcal{C}})$$

The nominal coding gain for Λ / Λ' is

$$\begin{aligned} \varrho(\Lambda / \Lambda') &= \frac{\omega_{\min}(\tilde{\mathcal{C}})}{(V(\mathcal{V}(\Lambda)))^{\frac{1}{n}}} \\ &= \frac{\omega_{\min}(\tilde{\mathcal{C}}) \prod_{\ell=1}^m |p_\ell|^{2 \sum_{t=0}^{\gamma_\ell-1} (\gamma_\ell - t) \frac{k'_{\ell,t}}{n}}}{v |\varpi|^2} \end{aligned} \quad (96)$$

The nominal coding gain of the EDC lattice in scenario 2 is related to the minimum Euclidean weight of the composite code $\tilde{\mathcal{C}}$ and the code rates of all nested linear codes at each layer.